SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 May 2026

Generated on 20 May 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-2026-34234	CtrlPanel is open-source billing software for hosting providers. In versions 1.1.1 and prior, the web-based installer (public/installer/index.php) is vulnerable to unauthenticated Remote Code Execution (RCE) because it performs the install.lock check only after including and executing form handler files, leaving installer endpoints reachable on already-installed instances. The handlers also pass unsanitized user input directly into shell commands, allowing an attacker to submit crafted requests that execute arbitrary commands on the server. The vulnerability stems from two combined weaknesses: (1) premature form handler execution before the lock file gate, and (2) unsafe use of user input in shell command construction. This issue is reported to be actively exploited in the wild. The issue has been fixed in version 1.2.0.	10.0	More Details
CVE-2026-44006	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, It is possible to reach BaseHandler.getPrototypeOf, which can be used to get arbitrary prototypes. This vulnerability is fixed in 3.11.0.	10.0	More Details
CVE-2026-41553	PDF Export Module used in DHTMLX's products Gantt and Scheduler is vulnerable to Remote Code Execution due to lack of "data" parameter sanitization. An unauthenticated attacker can inject the malicious JavaScript code to the parameter whose value is processed by Node.js and subsequently executed. This can lead to server compromise. This issue was fixed in PDF Export Module version 0.7.6.	10.0	More Details
CVE-2026-44523	Note Mark is an open-source note-taking application. Prior to 0.19.4, no minimum length or entropy is enforced on the JWT_SECRET configuration value. The application accepts any base64-decodable secret regardless of size, including secrets as short as 1 byte. This vulnerability is fixed in 0.19.4.	10.0	More Details
CVE-2026-20182	May 2026: This security advisory provides the details and fix information for a vulnerability that was discovered and fixed after the was disclosed in February 2026. This new advisory is for a new vulnerability in the control connection handshaking. The section of this advisory includes Show Control Connections guidance to help with system checks. A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system. This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to the affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.	10.0	More Details
CVE-2026-43633	HestiaCP versions 1.9.0 through 1.9.4 contain a deserialization vulnerability in the web terminal component caused by a session format mismatch between PHP and Node.js that allows unauthenticated remote attackers to achieve root-level code execution. Attackers can inject crafted data into HTTP headers that are processed by the PHP session handler but incorrectly deserialized by the Node.js web terminal component as trusted session values, resulting in arbitrary command execution on systems with the web terminal feature enabled.	10.0	More Details
CVE-2026-42822	Improper authentication in Azure Local Disconnected Operations allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-44005	vm2 is an open source vm/sandbox for Node.js. From 3.9.6 to 3.10.5, vm2's bridge exposes mutable proxies for real host-realm intrinsic prototypes and then forwards sandbox writes into the underlying host objects with otherReflectSet() and otherReflectDefineProperty(), which lets attacker-controlled JavaScript running in a default VM or inherited NodeVM mutate shared host Object.prototype, Array.prototype, and Function.prototype from inside the sandbox This vulnerability is fixed in 3.11.0.	10.0	More Details
CVE-2026-43997	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, it is possible to obtain the host Object. There are various ways to use the host Object, to escape the sandbox, one example would be using HostObject.getOwnPropertySymbols to obtain Symbol(nodejs.util.inspect.custom). This vulnerability is fixed in 3.11.0.	10.0	More Details

CVE-2026-27130	Dokploy is a free, self-hostable Platform as a Service (PaaS). Versions 0.26.6 and below have OS command injection through the appName parameter. 3 chained issues cause this problem: inadequate input sanitization, lack of schema validation and direct shell interpolation. User-controlled application names are passed through inadequate sanitization (cleanAppName function only replaces spaces and converts to lowercase) before being interpolated directly into shell commands executed via execAsync() and execAsyncRemote(). An authenticated attacker can inject shell metacharacters (e.g., ;, $(), backticks, |, &) in the appName field during application creation, which are then executed with server-level privileges when service operations (start, stop, remove, scale) are triggered. This issue has been resolved in version 0.26.7.	9.9	More Details
CVE-2026-33642	Kitty is a cross-platform GPU based terminal. In versions 0.46.2 and below, the handle_compose_command() function in kitty/graphics.c performs bounds validation on composition offsets using unsigned 32-bit arithmetic that is subject to integer wrapping, potentially leading to Heap Buffer Over-Read/Write. An attacker who can write escape sequences to a kitty terminal (e.g., via a malicious file, SSH login banner, or piped content) can supply crafted x_offset/y_offset values that pass the bounds check after wrapping but cause massive out-of-bounds heap memory access in compose_rectangles(). No user interaction is required. No non-default configuration is required. The attacker only needs the ability to produce output in a kitty terminal window. This issue has been fixed in version 0.47.0.	9.9	More Details
CVE-2026-44774	Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.46, 3.6.17, and 3.7.1, Traefik's Kubernetes Gateway API provider allows a tenant with HTTPRoute creation permissions to expose the REST provider handler, bypassing the providers.rest.insecure=false setting. The Gateway provider accepts any TraefikService backend reference whose name ends with @internal, making it possible to route traffic to rest@internal in addition to the intended api@internal. In shared Gateway deployments where the REST provider is enabled, this allows a low-privileged actor to gain live dynamic configuration write access to Traefik, enabling unauthorized reconfiguration of routers and services. This vulnerability is fixed in 2.11.46, 3.6.17, and 3.7.1.	9.9	More Details
CVE-2026-44442	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 16.9.1, certain endpoints failed to enforce proper authorization checks, allowing users to modify data beyond their permitted role. This vulnerability is fixed in 16.9.1.	9.9	More Details
CVE-2026-41050	Fleet's Helm deployer did not fully apply ServiceAccount impersonation in two code paths, allowing a tenant with git push access to a Fleet-monitored repository to read secrets from any namespace on every downstream cluster targeted by their `GitRepo`.	9.9	More Details
CVE-2026-43999	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, NodeVM's builtin allowlist can be bypassed when the module builtin is allowed (including via the '*' wildcard). The module builtin exposes Node's Module._load(), which loads any module by name directly in the host context, completely bypassing vm2's builtin restriction. This allows sandboxed code to load excluded builtins like child_process and achieve remote code execution. This vulnerability is fixed in 3.11.0.	9.9	More Details
CVE-2026-4883	The Piotnet Forms plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the 'piotnetforms_ajax_form_builder' function in all versions up to, and including, 2.1.40. The plugin uses an incomplete extension blacklist that only blocks php, phpt, php5, php7, and exe extensions, while allowing dangerous extensions such as .phar or .phtml to be uploaded. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The exploit can only be exploited if a file field is added to the form.	9.8	More Details
CVE-2018-25320	ACL Analytics versions 11.x through 13.0.0.579 contain an arbitrary code execution vulnerability that allows attackers to execute arbitrary commands by leveraging the EXECUTE function. Attackers can use bitsadmin to download malicious PowerShell scripts and execute them with system privileges to establish reverse shells and gain complete system control.	9.8	More Details
CVE-2026-8975	Memory safety bugs present in Thunderbird 140.10 and Thunderbird 150. 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 was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.8	More Details
CVE-2026-36829	An authentication bypass vulnerability exists in the embedded HTTP server of Panabit PAP-XM320 up to and including v7.7. The server validates session cookies using a filesystem existence check based on a user-controlled cookie value without proper sanitization, allowing directory traversal and bypass of authentication.	9.8	More Details
CVE-2026-45772	Turborepo is a high-performance build system for JavaScript and TypeScript codebases. From 1.1.0 to before 2.9.14, Turborepo can be vulnerable to arbitrary code execution when run in untrusted repositories that contain malicious Yarn configuration. In affected versions, package manager detection executed yarn --version from the project directory, which could cause Yarn to load and execute a project-controlled yarnPath from .yarnrc.yml. An attacker who controls repository contents could cause code execution when a user or CI system runs affected turbo, @turbo/codemod, or @turbo/workspace conversion commands. This vulnerability is fixed in 2.9.14.	9.8	More Details
CVE-2026-44717	MCP Calculate Server is a mathematical calculation service based on MCP protocol and SymPy library. Prior to 0.1.1, the use of eval() to evaluate mathematical expressions without proper input sanitization leads to remote code execution. This vulnerability is fixed in 0.1.1.	9.8	More Details
CVE-2026-8974	Memory safety bugs present in Thunderbird 140.10 and Thunderbird 150. 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 was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.8	More Details
CVE-2026-8973	Memory safety bugs present in Thunderbird 150. 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 was fixed in Firefox 151 and Thunderbird 151.	9.8	More Details
CVE-2021-47965	WordPress Plugin WP Super Edit 2.5.4 and earlier contains an unrestricted file upload vulnerability in the FCKeditor component that allows attackers to upload dangerous file types without validation. Attackers can upload arbitrary files through the filemanager upload endpoint to achieve remote code execution and complete system compromise.	9.8	More Details
CVE-2026-46364	phpMyFAQ before 4.1.2 contains an unauthenticated SQL injection vulnerability in BuiltinCaptcha::garbageCollector() and BuiltinCaptcha::saveCaptcha() methods that interpolate unsanitized User-Agent headers into DELETE and INSERT queries. Unauthenticated attackers can exploit the public GET /api/captcha endpoint by crafting malicious User-Agent headers to perform time-based blind SQL injection, extracting sensitive data including user credentials, admin tokens, and SMTP credentials from the database.	9.8	More Details
CVE-2020-37228	iDS6 DSSPro Digital Signage System 6.2 contains a CAPTCHA security bypass vulnerability that allows attackers to bypass authentication by requesting the autoLoginVerifyCode object. Attackers can retrieve valid CAPTCHA codes via the login endpoint and use them to perform brute-force attacks against user accounts.	9.8	More Details

CVE-2020-37239	libbabl 0.1.62 contains a broken double free detection vulnerability that allows attackers to bypass memory safety checks by exploiting signature overwriting in freed chunks. Attackers can call babl_free() twice on the same pointer without triggering detection, as libc's malloc metadata overwrites babl's signature field upon freeing, enabling potential memory corruption and code execution.	9.8	More Details
CVE-2021-47952	python jsonpickle 2.0.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary Python commands by deserializing malicious JSON payloads containing py/repr objects. Attackers can craft JSON strings with py/repr directives that invoke the eval function during deserialization to execute system commands and arbitrary code.	9.8	More Details
CVE-2018-25332	GitBucket 4.23.1 contains an unauthenticated remote code execution vulnerability that allows attackers to execute arbitrary commands by exploiting weak secret token generation and insecure file upload functionality. Attackers can brute-force the Blowfish encryption key, upload a malicious JAR plugin via the git-lfs endpoint, and execute system commands through an exposed exploit endpoint.	9.8	More Details
CVE-2026-4885	The Piotnet Addons for Elementor Pro plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the 'pafe_ajax_form_builder' function in all versions up to, and including, 7.1.70. The plugin uses an incomplete extension blacklist that only blocks php, phpt, php5, php7, and exe extensions, while allowing dangerous extensions such as .phar or .phtml to be uploaded. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The exploit can only be exploited if a file field is added to the form.	9.8	More Details
CVE-2018-25335	WordPress Plugin Peugeot Music 1.0 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by sending POST requests to the upload.php endpoint. Attackers can upload files with arbitrary extensions by manipulating the 'name' parameter to execute code from the uploads directory.	9.8	More Details
CVE-2026-8507	Crypt::OpenSSL::PKCS12 versions through 1.94 for Perl have out-of-bounds (OOB) write flaws. When parsing a PKCS12 file, with a >= 1 GiB OCTET STRING (or BIT STRING) attribute on a SAFEBAG, via info() or info_as_hash(), a heap out-of-bounds write would be triggered with remote-code-execution potential (RCE) due to a signed integer overflow in the size calculation passed to Renew().	9.8	More Details
CVE-2026-44159	Tyler Identity Local (TID-L) uses documented, default administrative credentials. Users are not required to change the credentials before deployment. TID-L has not been distributed since December 2020, and has not been supported since 2021.	9.8	More Details
CVE-2026-7301	SGLangs multimodal generation runtime scheduler's ROUTER socket binds to 0.0.0.0 by default and contains a sink that calls pickle.loads() on incoming messages, enabling RCE when exposed to the internet.	9.8	More Details
CVE-2026-7304	SGLangs multimodal generation runtime is vulnerable to unauthenticated remote code execution when the --enable-custom-logit-processor option is enabled, as Python objects loaded via dill.loads() will be deserialized without validation.	9.8	More Details
CVE-2026-8956	Integer overflow in the Networking: JAR component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.8	More Details
CVE-2026-5229	The Form Notify plugin for WordPress is vulnerable to Authentication Bypass in versions up to and including 1.1.10. This is due to the plugin trusting user-controlled cookie data to determine which WordPress account to authenticate after a LINE OAuth login. When LINE doesn't provide an email address (which is common), the plugin falls back to reading the 'form_notify_line_email' cookie value without verifying that the LINE account is associated with that email address. This makes it possible for unauthenticated attackers to gain access to any user account on the site, including administrator accounts, by completing a LINE OAuth flow with their own LINE account while injecting a malicious cookie containing the target victim's email address.	9.8	More Details
CVE-2026-8836	A vulnerability was found in lwIP up to 2.2.1. Affected is the function snmp_parse_inbound_frame of the file src/apps/snmp/snmp_msg.c of the component snmpv3 USM Handler. Performing a manipulation of the argument msgAuthenticationParameters results in stack-based buffer overflow. The attack may be initiated remotely. The patch is named 0c957ec03054eb6c8205e9c9d1d05d90ada3898c. It is suggested to install a patch to address this issue.	9.8	More Details
CVE-2026-25244	WebdriverIO is a test automation framework for unit, e2e and component testing using WebDriver, WebDriver BiDi and Appium. Versions below 9.24.0 contain a command injection vulnerability leading to remote code execution (RCE) in test orchestration. Git permits branch names containing shell metacharacters, and getGitMetadataForAISelection() interpolates these names directly into execSync() calls without sanitization. An attacker can exploit this by supplying a malicious repository (via testOrchestrationOptions.runSmartSelection.source, or the current directory if unset) whose branch name carries a payload, causing the shell to execute arbitrary code. This enables remote code execution on CI/CD servers and developer machines, leading to credential and secret disclosure, source code and SSH key exfiltration, system compromise, and supply chain attacks via tampered build artifacts. The issue has been fixed in version 9.24.0.	9.8	More Details
CVE-2026-8838	Unsafe use of Python's eval() on server-received data in the vector_in() function in amazon-redshift-python-driver before 2.1.14 allows a rogue server or man-in-the-middle actor to execute arbitrary code on the client. To remediate this issue, users should upgrade to version 2.1.14.	9.8	More Details
CVE-2026-8721	Crypt::OpenSSL::PKCS12 versions through 1.94 for Perl truncates passwords with embedded NULLs. Password parameters in PKCS12.xs are declared char *, which routes through Perl's default typemap to SvPV_nolen. The Perl length is discarded. The C code (or OpenSSL internally) calls strlen() on the buffer. Any password byte at or after the first NULL is silently dropped. Binary / KDF-derived / HMAC-derived passwords lose entropy without any warnings.	9.8	More Details
CVE-2026-8398	A supply chain attack compromised the official installation packages of DAEMON Tools Lite (Windows versions 12.5.0.2421 through 12.5.0.2434), distributed from the legitimate website daemon-tools.cc between approximately April 8, 2026, and May 5, 2026. Attackers gained unauthorized access to the vendor's (AVB Disc Soft) build or distribution infrastructure and trojanized three binaries: DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe. These files were digitally signed with the legitimate AVB Disc Soft code-signing certificate, allowing the malicious installers to appear trustworthy and bypass signature-based detection.	9.8	More Details
CVE-2026-2347	Authorization bypass through User-Controlled key vulnerability in Akilli Commerce Software Technologies Ltd. Co. E-Commerce Website allows Session Hijacking. This issue affects E-Commerce Website: before 4.5.001.	9.8	More Details
CVE-2026-44009	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.2, This vulnerability is fixed in 3.11.2.	9.8	More Details

CVE-2020-37168	Ecommerce Systempay 1.0 contains a weak cryptographic implementation vulnerability that allows attackers to brute force the 16-character production secret key used for payment signature generation. Attackers can extract payment form data and signatures from POST requests to the payment endpoint, then use SHA1 hash comparison to iteratively test key candidates until discovering the correct production key, enabling them to forge valid payment signatures and manipulate transaction amounts.	9.8	More Details
CVE-2026-26191	Fleet is open source device management software. Prior to version 4.81.0, a vulnerability in Fleet's software installer pipeline could allow a crafted software package to execute arbitrary commands as root (macOS/Linux) or SYSTEM (Windows) on managed endpoints when an uninstall is triggered. When a software package (.pkg, .deb, .rpm, .exe, or .msi) is uploaded to Fleet, metadata is extracted from the package binary and used to generate uninstall scripts. In affected versions, this metadata is not properly sanitized before being included in the generated scripts. A specially crafted package containing malicious values in its metadata fields could result in unintended command execution when the uninstall script runs on managed endpoints. Version 4.81.0 contains a patch. If an immediate upgrade is not possible, administrators should avoid uploading software packages obtained from untrusted or unverified sources. Additionally, administrators can manually inspect and edit auto-generated uninstall scripts before deployment.	9.8	More Details
CVE-2026-42031	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.10 and 2.11.5, a vulnerability in datastore_search_sql allowed attackers to inject SQL in order to gain access to private resources and PostgreSQL system information This vulnerability is fixed in 2.10.10 and 2.11.5.	9.8	More Details
CVE-2026-8500	Web::Passwd versions through 0.03 for Perl is vulnerable to RCE. Web::Passwd is a small CGI application for managing htpasswd files using the htpasswd command. The user parameter is not validated or escaped, and is used as the last argument on the command line, allowing for command injection.	9.8	More Details
CVE-2026-8181	The Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative) plugin for WordPress is vulnerable to Authentication Bypass in versions 3.4.0 to 3.4.1.1. This is due to incorrect return-value handling in the `is_mainwp_authenticated()` function when validating application passwords from the Authorization header. This makes it possible for unauthenticated attackers, with knowledge of an administrator username, to impersonate that administrator for the duration of the request by supplying any random Basic Authentication password achieving privilege escalation.	9.8	More Details
CVE-2026-6271	The Career Section plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.7 via the CV upload handler. This is due to missing file type validation. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.	9.8	More Details
CVE-2026-6510	The InfusedWoo Pro plugin for WordPress is vulnerable to privilege escalation via missing authorization in all versions up to, and including, 5.1.2. This is due to missing nonce verification and capability checks in the iwar_save_recipe() AJAX handler. This makes it possible for unauthenticated attackers to create a malicious automation recipe that pairs an HTTP post trigger with an auto-login action, allowing any unauthenticated visitor to visit a crafted URL and receive authentication cookies for any targeted user account (e.g., administrator), achieving complete authentication bypass and privilege escalation.	9.8	More Details
CVE-2026-45411	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.3, it is possible to catch a host exception using the yield* expression inside an async generator. When the generator is closed using the return function, the value is awaited on and exceptions thrown in the then call will be caught by the runtime and passed to the yield* iterator as the next value. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This vulnerability is fixed in 3.11.3.	9.8	More Details
CVE-2026-42589	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, Gotenberg's /forms/pdfengines/metadata/write HTTP endpoint accepts a JSON metadata object and passes its keys directly to ExifTool via the go-exiftool library. No validation is performed on key characters. A \n embedded in a JSON key splits the ExifTool stdin stream into a new argument line, allowing an attacker to inject arbitrary ExifTool flags — including -if, which evaluates Perl expressions. This achieves unauthenticated OS command execution in a single HTTP request. The response is HTTP 200 with a valid PDF, making the attack transparent to basic monitoring. This vulnerability is fixed in 8.31.0.	9.8	More Details
CVE-2026-44008	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.2, the new method neutralizeArraySpeciesBatch works with objects from the other side but can call into this side via getter on the array prototype exposing objects of the wrong side into the sandbox. This can be used to get host objects and get the host Function object. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This vulnerability is fixed in 3.11.2.	9.8	More Details
CVE-2025-11024	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Akilli Commerce Software Technologies Ltd. Co. E-Commerce Website allows Blind SQL Injection. This issue affects E-Commerce Website: before 4.5.001.	9.8	More Details
CVE-2026-8953	Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.6	More Details
CVE-2026-8580	Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-8959	Sandbox escape due to incorrect boundary conditions in the Widget: Win32 component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.6	More Details
CVE-2026-8511	Use after free in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-44482	soundcloud-rpc is a SoundCloud Client with Discord Rich Presence, Dark Mode, Last.fm and AdBlock support. Prior to 0.1.8, a track title containing an HTML payload executed locally in the Electron app. This means attacker-controlled SoundCloud track metadata can lead to local command execution on the user's machine. The application exposes a preload API (window.soundcloudAPI.sendTrackUpdate) to the remote SoundCloud page. Track metadata from SoundCloud is trusted and forwarded through IPC into the Electron main process. The app later renders that metadata as raw HTML inside privileged Electron views that have Node.js integration enabled. This vulnerability is fixed in 0.1.8.	9.6	More Details
CVE-2026-2587	A critical Remote Code Execution (RCE) vulnerability was identified in the server-side template rendering mechanism used by the Glassfish gadget handler. The application processes .xml files and evaluates user-supplied values within a context where Expression Language (EL) “expressions” are processed without proper sanitization or escaping. By injecting expressions such as #{7*7}, the server returns 49, confirming server-side EL evaluation. This issue allows a remote attacker to fully	9.6	More Details

	compromise the underlying host, enabling capabilities as reading/modifying data, executing arbitrary commands, persistence, and lateral movement.		
CVE-2026-41615	Exposure of sensitive information to an unauthorized actor in Microsoft Authenticator allows an unauthorized attacker to disclose information over a network.	9.6	More Details
CVE-2026-47107	Windmill prior to 1.703.2 contains an incorrect default permissions vulnerability in nsjail sandbox configuration files where /etc is bind-mounted without read-write restrictions, allowing authenticated users to write arbitrary entries to /etc/hosts, /etc/resolv.conf, and /etc/ssl/certs/ca-certificates.crt from within script execution sandboxes. Attackers can exploit persistent poisoned entries across all subsequent script executions on the same worker pod to redirect hostnames, intercept DNS queries, perform transparent HTTPS man-in-the-middle attacks, and intercept WM_TOKEN JWTs to gain workspace-admin access to victim workspaces across tenants.	9.6	More Details
CVE-2026-44592	Gradient is a nix-based continuous integration system. In 1.1.0, when GRADIENT_DISCOVERABLE=true (the default, and the NixOS module default), anyone who can reach /proto can register as a worker without any credentials by sending a fresh, never-registered worker UUID. The resulting session has PeerAuth::Open, i.e. it sees jobs from every organisation, and can immediately NarPush/NarUploaded arbitrary store paths into nar_storage and the cached_path table. This vulnerability is fixed in 1.1.1.	9.4	More Details
CVE-2026-42596	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, the default deny-lists used by Gotenberg's downloadFrom feature and webhook feature are bypassable. Because the filter is regex-based and case-sensitive, an unauthenticated attacker can supply URLs such as http://[::ffff:127.0.0.1]:... and reach loopback or private HTTP services that the default deny-list is intended to block. This crosses a real security boundary because an external caller can force the server to make outbound requests to internal-only targets. This vulnerability is fixed in 8.31.0.	9.4	More Details
CVE-2026-8950	Same-origin policy bypass in the Networking: HTTP component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	9.3	More Details
CVE-2026-44212	PrestaShop is an open source e-commerce web application. Prior to 8.2.6 and 9.1.1, there is a stored Cross-Site Scripting (XSS) vulnerability in the PrestaShop back-office Customer Service view. An unauthenticated attacker can submit the public Contact Us form with a malicious email address. The payload is stored in the database and executed when a back-office employee opens the affected customer thread, enabling session hijacking and full back-office takeover. This vulnerability is fixed in 8.2.6 and 9.1.1.	9.3	More Details
CVE-2025-27851	The locally served web site on the Garmin WDU (v1 1.4.6 and v2 5.0) allows a cross-site origin WebSocket hijacking attack. Among other uses, the WDU utilizes WebSockets to control settings, including administrative settings. This allows a network attacker to take full control of a WDU. To initiate an exploit of this vulnerability, the victim must (1) be utilizing a web browser on a multihomed host that has local interfaces on the Garmin Marine Network as well as another network, and (2) access a malicious third party website created by the attacker.	9.3	More Details
CVE-2026-41225	A vulnerability exists in iControl REST where a highly privileged, authenticated attacker with at least the Manager role can create configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	9.1	More Details
CVE-2026-44007	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.1, when a NodeVM is created with nesting: true, sandbox code can unconditionally require('vm2') regardless of the outer VM's require configuration — including require: false. With access to vm2, the sandbox constructs a new inner NodeVM with its own unrestricted require settings and executes arbitrary OS commands on the host. Any application that runs untrusted code inside a NodeVM with nesting: true is fully compromised. This vulnerability is fixed in 3.11.1.	9.1	More Details
CVE-2026-2586	An authenticated Remote Code Execution (RCE) vulnerability was identified in GlassFish's Administration Console. A user with access to the panel can send crafted requests that allow the execution of arbitrary operating system commands with the privileges of the application service user.	9.1	More Details
CVE-2026-8948	Same-origin policy bypass in the DOM: Networking component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	9.1	More Details
CVE-2026-42032	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.10 and 2.11.5, a vulnerability in datastore_search_sql allowed attackers to bypass authorization in order to gain access to private resources and PostgreSQL system information This vulnerability is fixed in 2.10.10 and 2.11.5.	9.1	More Details
CVE-2026-44351	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.2.4, a critical authentication-bypass vulnerability in fast-jwt's async key-resolver flow allows any unauthenticated attacker to forge arbitrary JWTs that are accepted as authentic. When the application's key resolver returns an empty string (''), for example via the common keys[decoded.header.kid] || '' JWKS-style fallback, fast-jwt converts it to a zero-length Buffer, hands it to crypto.createSecretKey, derives allowedAlgorithms = ['HS256','HS384','HS512'] from it, and then verifies the token's signature against an empty-key HMAC. The attacker simply computes HMAC-SHA256(key='', input='${header}.${payload}'), which Node accepts without complaint — and the verifier returns the attacker-chosen payload (sub, admin, scopes, etc.) as authentic. This vulnerability is fixed in 6.2.4.	9.1	More Details
CVE-2026-41919	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	9.1	More Details
CVE-2026-31986	Use of Hard-coded Cryptographic Key vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	9.1	More Details
CVE-2023-24215	Incorrect access control in the /uci/get/ endpoint of NOVUS AirGate 4G firmware v1.1.16 allows unauthenticated attackers to obtain administrator credentials via a crafted POST request.	9.1	More Details
CVE-2026-44377	CubeCart is an ecommerce software solution. Prior to 6.7.0, an Authenticated Server-Side Template Injection (SSTI) vulnerability exists in multiple modules of CubeCart (including Email Templates and Documents). The application unsafely evaluates user-supplied input directly through the Smarty template engine. By leveraging this, an authenticated attacker with administrative privileges can bypass current restrictions and call native PHP functions within the templates, such as readgzfile() to read sensitive configuration files, or error_log() to write a malicious PHP web shell, ultimately achieving Information Disclosure and full Remote Code Execution (RCE). This vulnerability is fixed in 6.7.0.	9.1	More Details
	CubeCart is an ecommerce software solution. Prior to 6.7.0, an Authenticated Arbitrary File Upload vulnerability exists in the REST API File Manager endpoint (POST /api/v1/files) of CubeCart. The endpoint allows any holder of an API key with files:rw		

CVE-2026-45053	permission to upload PHP source files into the web-accessible images/source/ directory, where they are executed by the web server. Combined with a path-traversal flaw in the same endpoint's filepath parameter, a single API request writes a webshell anywhere the webserver process can write — including the document root — yielding full Remote Code Execution. This vulnerability is fixed in 6.7.0.	9.1	More Details
CVE-2026-8634	Crabbox prior to v0.12.0 contains an environment variable exposure vulnerability that allows attackers with access to a malicious or compromised repository to forward local secrets such as API tokens, cloud credentials, and broker tokens into the remote command environment. Attackers can exploit overly permissive environment variable allowlisting in repo-local Crabbox configuration to serialize sensitive environment variables into remote command execution, exposing credentials to the remote environment.	9.1	More Details
CVE-2026-44542	FileBrowser Quantum is a free, self-hosted, web-based file manager. Prior to 1.3.1-stable and 1.3.9-beta, attacker-controlled path input is joined with a trusted base path prior to sanitization, allowing traversal sequences (e.g., ../) to escape the intended shared directory. As a result, an unauthenticated attacker possessing a valid public share hash with delete permissions enabled can delete arbitrary files outside the shared directory within the share owner’s configured storage scope. This affects public/api/resources and public/api/resources/bulk. This vulnerability is fixed in 1.3.1-stable and 1.3.9-beta.	9.1	More Details
CVE-2026-41258	OpenMRS is an open source electronic medical record system platform. From 2.7.0 to before 2.7.9 and 2.8.6, the ConceptReferenceRangeUtility.evaluateCriteria() method in OpenMRS Core evaluates database-stored criteria strings as Apache Velocity templates without any sandbox configuration. The VelocityEngine is initialized with only logging properties and noSecureUberspector, leaving the default UberspectImpl in place, which allows unrestricted Java reflection through template expressions. A user with the Manage Concepts privilege can store a malicious Velocity template expression in a concept's reference range criteria field. This payload is then executed automatically whenever a user or API call validates an observation against the affected concept. The Velocity context exposes $patient (the Person / Patient object), $obs (the Obs object), and $fn (the ConceptReferenceRangeUtility instance with access to the full OpenMRS service layer). This vulnerability is fixed in 2.7.9 and 2.8.6.	9.1	More Details
CVE-2026-42555	Valtimo is an open-source business process automation platform. com.ritense.valtimo:document from 12.0.0 to before 12.32.0, com.ritense.valtimo:case from 13.0.0 to before 13.23.0, and com.ritense.valtimo:contract from 13.4.0 to before 13.23.0 evaluate Spring Expression Language (SpEL) expressions from user-supplied input using StandardEvaluationContext, which provides unrestricted access to Java types and methods. An authenticated user with the ADMIN role can achieve Remote Code Execution and credential exfiltration. This vulnerability is fixed in com.ritense.valtimo:document 2.32.0, com.ritense.valtimo:case 13.23.0, and com.ritense.valtimo:contract 13.23.0.	9.1	More Details
CVE-2026-45010	phpMyFAQ before 4.1.2 contains an improper restriction of excessive authentication attempts vulnerability in the /admin/check endpoint, which accepts arbitrary user-id parameters without session binding or rate limiting. Unauthenticated attackers can brute-force any user's six-digit TOTP code by submitting POST requests with sequential token values, bypassing two-factor authentication to gain full administrative access.	9.1	More Details
CVE-2026-44551	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the LDAP authentication endpoint does not validate that the submitted password is non-empty before performing a Simple Bind against the LDAP server. The LdapForm Pydantic model accepts password: str with no minimum length constraint, so an empty string passes validation. The subsequent Connection.bind() call succeeds on vulnerable LDAP servers, and the application issues a full session token for the target user. This vulnerability is fixed in 0.9.0.	9.1	More Details
CVE-2025-11159	Hitachi Vantara Pentaho Data Integration & Analytics of all versions contain a JDBC driver for H2 databases which is vulnerable to external script execution when a new connection is created by a data source administrator.	9.1	More Details
CVE-2026-6512	The InfusedWoo Pro plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.1.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to permanently delete arbitrary posts, pages, products, or orders, mass-delete all comments on any post, and change any post's status.	9.1	More Details
CVE-2026-7302	SGLangs multimodal generation runtime is vulnerable to an unauthenticated path traversal vulnerability, allowing an attacker to write arbitrary files anywhere the server process has write access, by including ../ sequences in the upload filename when sent to specific endpoints.	9.1	More Details
CVE-2026-45158	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.8, unsanitized user input is passed to the DHCP configuration of the configured interface, which is processed by a shell script, allowing remote code execution as root on the underlying operating system. This vulnerability is fixed in 26.1.8.	9.1	More Details
CVE-2026-44194	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.8, an authenticated Remote Code Execution (RCE) vulnerability in the OPNsense core allows a user with user-management privileges to execute arbitrary system commands as root. An attacker can bypass input validation by formatting their malicious payload as a compliant email address, allowing shell commands to reach the underlying operating system. The flaw exists in the local user synchronization flow, within core/src/opnsense/scripts/auth/sync_user.php. This vulnerability is fixed in 26.1.8.	9.1	More Details
CVE-2026-45230	DumbAssets through 1.0.11 contains a path traversal vulnerability in the POST /api/delete-file endpoint and filesToDelete array parameters that allows unauthenticated attackers to delete arbitrary files by supplying ../ sequences that bypass directory boundary validation. Attackers can exploit the optional and disabled-by-default authentication control to traverse outside the intended application directory and delete critical files such as server.js or package.json, causing complete denial of service.	9.1	More Details
CVE-2026-44193	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.7, the XMLRPC method opnsense.restore_config_section fails to sanitize user supplied input leading to Remote Code Execution. This vulnerability is fixed in 26.1.7.	9.1	More Details
CVE-2026-45714	CubeCart is an ecommerce software solution. Prior to 6.7.0, an Authenticated Server-Side Template Injection (SSTI) vulnerability exists in multiple modules of CubeCart (including Email Templates, Invoices, Documents, and Contact Forms). The application unsafely evaluates user-supplied input using the Smarty template engine without enabling Smarty Security Policies. This allows any authenticated user with administrative privileges to execute arbitrary operating system commands (RCE) on the server. This vulnerability is fixed in 6.7.0.	9.1	More Details
	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, SiYuan's Bazaar (community marketplace) renders the name and version fields of a package's plugin.json (and the equivalent theme.json / template.json / widget.json /		

CVE-2026-45375	icon.json) into the Settings → Marketplace UI without HTML escaping. The kernel-side helper sanitizePackageDisplayStrings in kernel/bazaar/package.go HTML-escapes only Author, DisplayName, and Description — Name and Version flow through to the renderer raw. The frontend at app/src/config/bazaar.ts substitutes them into HTML template strings via ${item.preferredName} / ${data.name} / v${data.version} and assigns the result to innerHTML. As a consequence, malicious HTML in either field is parsed and executed when a user opens the marketplace tab. This vulnerability is fixed in 3.7.0.	9.0	More Details
CVE-2026-42457	vCluster Platform provides a Kubernetes platform for managing virtual clusters, multi-tenancy, and cluster sharing. Prior to 4.4.3, 4.5.5, 4.6.2, 4.7.1, and 4.8.0, there is a Stored XSS attack vulnerability via the name field of a templateRef. This can lead to the execution of arbitrary external scripts within the platform's browser context. In the worst case, a malicious user could potentially create a new Global-Admin user, bypassing other security restrictions. The attacker needs the ability to create namespaces. This vulnerability is fixed in 4.4.3, 4.5.5, 4.6.2, 4.7.1, and 4.8.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-3425	The RTMKit Addons for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0.2 via the 'path' parameter of the 'get_content' AJAX action. 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 files can be uploaded and included.	8.8	More Details
CVE-2021-47964	Schlix CMS 2.2.6-6 contains a remote code execution vulnerability that allows authenticated attackers to execute arbitrary PHP code by uploading malicious extension packages through the block manager. Attackers can upload a crafted ZIP file containing PHP code in the packageinfo.inc file and trigger execution by accessing the About tab of the installed extension.	8.8	More Details
CVE-2026-44827	Diffusers is the a library for pretrained diffusion models. Prior to 0.38.0, diffusers 0.37.0 allows remote code execution without the trust_remote_code=True safeguard when loading pipelines from Hugging Face Hub repositories. The _resolve_custom_pipeline_and_cls function in pipeline_loading_utils.py performs string interpolation on the custom_pipeline parameter using f"{custom_pipeline}.py". When custom_pipeline is not supplied by the user, it defaults to None, which Python interpolates as the literal string "None.py". If an attacker publishes a Hub repository containing a file named None.py with a class that subclasses DiffusionPipeline, the file is automatically downloaded and executed during a standard DiffusionPipeline.from_pretrained() call with no additional keyword arguments. The trust_remote_code check in DiffusionPipeline.download() is bypassed because it evaluates custom_pipeline is not None as False (since the kwarg was never supplied), while the downstream code path that actually loads the module resolves the None value into a valid filename. An attacker can achieve silent arbitrary code execution by publishing a malicious model repository with a None.py file and a standard-looking model_index.json that references a legitimate pipeline class name, requiring only that a victim calls from_pretrained on the repository. This vulnerability is fixed in 0.38.0.	8.8	More Details
CVE-2026-44513	Diffusers is the a library for pretrained diffusion models. Prior to 0.38.0, a trust_remote_code bypass in DiffusionPipeline.from_pretrained allows arbitrary remote code execution despite the user passing trust_remote_code=False (or omitting it, which is the default). The vulnerability has three variants, all sharing the same root cause — the trust_remote_code gate was implemented inside DiffusionPipeline.download() rather than at the actual dynamic-module load site, so any code path that bypassed or short-circuited download() also bypassed the security check. DiffusionPipeline.from_pretrained('repoA', custom_pipeline='attacker/repoB', trust_remote_code=False) — the gate evaluated against repoA's file list rather than repoB's, so repoB's pipeline.py was loaded and executed. DiffusionPipeline.from_pretrained('/local/snapshot', custom_pipeline='attacker/repoB', trust_remote_code=False) — the local-path branch never invoked download(), so the gate was never reached and remote code from repoB executed. DiffusionPipeline.from_pretrained('/local/snapshot', trust_remote_code=False) where the snapshot contains custom component files (e.g. unet/my_unet_model.py) referenced from model_index.json — same root cause; the local path skipped download() and custom component code executed. This vulnerability is fixed in 0.38.0.	8.8	More Details
CVE-2026-8524	Out of bounds write in WebAudio in Google Chrome prior to 148.0.7778.168 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-2026-8551	Use after free in Downloads in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-8549	Use after free in Media in Google Chrome prior to 148.0.7778.168 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-2026-32740	libheif is a HEIF and AVIF file format decoder and encoder. Versions 1.21.2 and prior contain a heap-buffer-overflow (write) vulnerability in the grid tile compositing, allowing an attacker to write 64 bytes of fully attacker-controlled data past the end of a chroma plane heap allocation by crafting a HEIF/AVIF file with a 1×4 grid of odd-height tiles. The overflow is triggered during normal image decoding with default build configuration. The written bytes are chroma (Cb/Cr) pixel values from the attacking tile, giving the attacker full control over the overflow content. This issue has been fixed in version 1.22.0.	8.8	More Details
CVE-2026-42559	RMCP is an official Rust SDK for the Model Context Protocol. Prior to version 1.4.0, the rmcp crate's Streamable HTTP server transport (crates/rmcp/src/transport/streamable_http_server/) did not validate the incoming Host header. This allowed a malicious public website, via a DNS rebinding attack, to send authenticated requests to an MCP server running on the victim's loopback or private-network interface. This vulnerability is fixed in 1.4.0.	8.8	More Details
CVE-2026-45672	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.12, the /api/v1/utils/code/execute endpoint executes arbitrary Python code via Jupyter for any verified user, even when the admin has set ENABLE_CODE_EXECUTION=false. The feature gate is not enforced on the API endpoint — the configuration says "disabled" but code still executes. This vulnerability is fixed in 0.8.12.	8.8	More Details
CVE-2026-6637	Stack buffer overflow in PostgreSQL module "refint" allows an unprivileged database user to execute arbitrary code as the operating system user running the database. A distinct attack is possible if the application declares a user-controlled column as a "refint" cascade primary key and facilitates user-controlled updates to that column. In that case, a SQL injection allows a primary key update value provider to execute arbitrary SQL as the database user performing the primary key update. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	8.8	More Details
	Use of inherently dangerous function PQfn(..., result_is_int=0, ...) in PostgreSQL libpq lo_export(), lo_read(), lo_lseek64(), and lo_tell64()		

CVE-2026-6477	functions allows the server superuser to overwrite a client stack buffer with an arbitrarily-large response. Like gets(), PQfn(..., result_is_int=0, ...) stores arbitrary-length, server-determined data into a buffer of unspecified size. Because both the \lo_export command in psql and pg_dump call lo_read(), the server superuser can overwrite pg_dump or psql stack memory. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	8.8	More Details
CVE-2026-6475	Symlink following in PostgreSQL pg_basebackup plain format and in pg_rewind allows an origin superuser to overwrite local files, e.g. /var/lib/postgres/.bashrc, that hijack the operating system account. It will remain the case that starting the server after these commands implicitly trusts the origin superuser, due to features like shared_preload_libraries. Hence, the attack has practical implications only if one takes relevant action between these commands and server start, like moving the files to a different VM or snapshotting the VM. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	8.8	More Details
CVE-2026-8581	Use after free in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-6473	Integer wraparound in multiple PostgreSQL server features allows an unprivileged database user to cause the server to undersize an allocation and write out-of-bounds. This may execute arbitrary code as the operating system user running the database. In applications that pass gigabyte-scale user inputs to the relevant database functions, the application input provider may achieve a segmentation fault. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	8.8	More Details
CVE-2025-15025	Authorization bypass through User-Controlled key vulnerability in Yordam Information Technology Consulting, Training and Electronic Systems Industry and Trade Inc. Library Automation System allows Exploitation of Trusted Identifiers. This issue affects Library Automation System: from v.21.6 before v.22.1.	8.8	More Details
CVE-2020-37227	HS Brand Logo Slider 2.1 contains an unrestricted file upload vulnerability that allows authenticated users to bypass client-side file extension validation by uploading arbitrary files. Attackers can intercept upload requests to the logoupload parameter in the admin interface and rename files to executable extensions .php to achieve remote code execution.	8.8	More Details
CVE-2025-15023	Incorrect Authorization vulnerability in Yordam Information Technology Consulting, Training and Electronic Systems Industry and Trade Inc. Library Automation System allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Library Automation System: from v.19.5 before v.22.1.	8.8	More Details
CVE-2026-45035	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.233, Tabby registers itself as the handler for the tabby:// URL scheme on all platforms. The URL scheme handler supports a run command that directly executes OS commands with no user confirmation, sanitization, or sandboxing. An attacker can craft a malicious link (tabby://run?command=...) and deliver it via a website, email, chat message, or any other medium. When a victim clicks the link, the OS launches Tabby which immediately spawns the specified command as a child process with the user's full privileges. This is a zero-click-after-link-visit RCE vulnerability. This vulnerability is fixed in 1.0.233.	8.8	More Details
CVE-2026-8544	Use after free in Media in Google Chrome prior to 148.0.7778.168 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-2025-15024	Improper Control of Generation of Code ('Code Injection') vulnerability in Yordam Information Technology Consulting, Training and Electronic Systems Industry and Trade Inc. Library Automation System allows Remote Code Inclusion. This issue affects Library Automation System: from v.19.5 before v.22.1.	8.8	More Details
CVE-2026-8577	Integer overflow in Fonts in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-8517	Object lifecycle issue in WebShare in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-45434	Improper Authentication vulnerability in Apache OFBiz via Password-Change Logic Flaw Leading to Remote Code Execution This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	8.8	More Details
CVE-2026-8509	Heap buffer overflow in WebML in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-41957	An authenticated remote code execution vulnerability through undisclosed vectors exists in the BIG-IP and BIG-IQ Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2026-43909	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, a signed 32-bit integer overflow in the loop index expression i * 4 inside SwapRGBABytes() causes the function to compute a large negative pointer offset when processing kABGR DPX images with large dimensions. The immediate crash is an out-of-bounds read (the memcpy at line 45 reads from &input[i * 4] first), but the subsequent write operations at lines 46–49 target the same wrapped offset — making this a combined OOB read+write primitive. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	8.8	More Details
CVE-2026-43908	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, a signed 32-bit integer overflow in the pixel-loop index expression i * 3 inside ConvertCbYCrYToRGB() causes the function to compute a large negative pointer offset into the output buffer, producing an out-of-bounds write that crashes the process. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	8.8	More Details
CVE-2026-8518	Use after free in Blink in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-42266	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. From 4.0.0 to 4.5.6, the allow-list of extensions that can be installed from PyPI Extension Manager (allowed_extensions_uris) is not correctly enforced by JupyterLab. The PyPI Extension Manager was not contained to packages listed on the default PyPI index. This vulnerability is fixed in 4.5.7.	8.8	More Details

CVE-2026-6228	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in versions up to and including 3.28.36. This is due to insufficient authorization checks in the role field update mechanism combined with overly permissive capabilities for the admin_form post type. The admin_form custom post type uses 'capability_type' => 'page', which grants editors the ability to create and edit forms. When an editor creates an edit_user form, they can manipulate the form configuration to include 'administrator' in the role_options array by directly submitting POST data to wp-admin/post.php, bypassing the UI restrictions in feadmin_get_user_roles(). When the form is subsequently submitted, the pre_update_value() function in class-role.php only validates that the submitted role exists in the form's role_options array (lines 107-110), but fails to verify that the current user has permission to assign that specific role. This makes it possible for unauthenticated attackers to first register as editors (via a public new_user form), then create an edit_user form with administrator in the allowed roles, and finally use that form to escalate their own privileges to administrator.	8.8	More Details
CVE-2026-8558	Out of bounds write in Fonts in Google Chrome prior to 148.0.7778.168 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-2026-27648	in OpenHarmony v6.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps.	8.8	More Details
CVE-2026-8621	Crabbox prior to v0.12.0 contains an authentication bypass vulnerability that allows non-admin shared-token callers to impersonate other owners or organizations by spoofing identity headers. Attackers can inject malicious X-Crabbox-Owner and X-Crabbox-Org headers in requests authenticated with a shared token to bypass authorization checks and access owner/org-scoped lease operations belonging to victim accounts.	8.8	More Details
CVE-2026-8555	Use after free in GTK in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-8519	Integer overflow in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2025-12008	Authorization bypass through User-Controlled key vulnerability in APPYAP Technology and Information Inc. Yaay Social Media App allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Yaay Social Media App: from 3.8.0 through 24102025.	8.8	More Details
CVE-2026-8587	Use after free in Extensions in Google Chrome on Mac prior to 148.0.7778.168 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-6506	The InfusedWoo Pro plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.1.2. This is due to the infusedwoo_gdpr_upddata() function missing authorization and capability checks, as well as lacking restrictions on which user meta keys can be updated. This makes it possible for authenticated attackers, with subscriber-level access and above, to update their own wp_capabilities user meta to grant themselves Administrator role privileges.	8.8	More Details
CVE-2026-3220	The Autoptimize WordPress plugin before 3.1.15, Clearfy Cache WordPress plugin before 2.4.2, Speed Optimizer WordPress plugin before 7.7.9 are vulnerable to unauthenticated Stored Cross-Site Scripting (XSS) due to a predictable replacement hash used during the HTML minification process and abusing a regular expression. This allows an attacker to inject arbitrary HTML attributes in the final HTML output by anticipating the placeholder format.	8.8	More Details
CVE-2026-8531	Heap buffer overflow in WebML in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-44293	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs generated JavaScript for toObject conversion could include an unsafe expression derived from a schema-controlled bytes field default value. A crafted descriptor with a non-string default value for a bytes field could cause attacker-controlled code to be emitted into the generated conversion function. This vulnerability is fixed in 7.5.6 and 8.0.2.	8.8	More Details
CVE-2026-6281	A potential vulnerability was reported in some Lenovo Personal Cloud Storage devices that could allow a remote authenticated user on the local network to execute arbitrary commands on the device.	8.8	More Details
CVE-2026-8529	Heap buffer overflow in Codecs in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted video file. (Chromium security severity: High)	8.8	More Details
CVE-2026-42550	Flight is an extensible micro-framework for PHP. Prior to 3.18.1, SimplePdo::insert(), SimplePdo::update(), and SimplePdo::delete() build SQL statements by concatenating the $table argument and the keys of the $data array directly into the query, with no identifier quoting and no validation. When an application forwards user-controlled data shapes to these helpers — a common and documented pattern, e.g. $db->insert('users', $request->data->getData()) — an attacker can inject arbitrary SQL by crafting malicious array keys. This vulnerability is fixed in 3.18.1.	8.8	More Details
CVE-2026-8775	A flaw has been found in Edimax BR-6428NS 1.10. This affects the function formL2TPSetup of the file /goform/formL2TPSetup of the component POST Request Handler. This manipulation of the argument L2TPUserName causes buffer overflow. 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.	8.8	More Details
CVE-2026-8776	A vulnerability has been found in Edimax BR-6428NS 1.10. This vulnerability affects the function formPPTPSetup of the file /goform/formPPTPSetup of the component POST Request Handler. Such manipulation of the argument pptpUserName leads to buffer overflow. 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.	8.8	More Details
CVE-2026-8527	Insufficient validation of untrusted input in Downloads in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-			

2026-8532	Integer overflow in XML in Google Chrome prior to 148.0.7778.168 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-2026-7498	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Basamak Information Technology Consulting and Organization Trade Ltd. Co. DernekWeb allows Stored XSS. This issue affects DernekWeb: through 30122025.	8.8	More Details
CVE-2026-8053	An issue in MongoDB Server's time-series collection implementation allows an authenticated user with database write privileges to trigger an out-of-bounds memory write in the mongod process. The issue results from an inconsistency in the internal field-name-to-index mapping within the time-series bucket catalog. Under certain conditions this can result in arbitrary code execution. This issue impacts MongoDB Server v5.0 versions prior to 5.0.33, v6.0 versions prior to 6.0.28, v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	8.8	More Details
CVE-2025-57282	ngrok v4.3.3 and 5.0.0-beta.2 is vulnerable to Command Injection.	8.8	More Details
CVE-2026-41085	Thermo Fisher Scientific Torrent Suite Dx through 5.14.2 has a privilege escalation vulnerability that may allow an authenticated user with limited access privileges to gain unauthorized administrator-level privileges through exploitation of specific system interfaces.	8.8	More Details
CVE-2026-45495	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	8.8	More Details
CVE-2026-36828	A command injection vulnerability exists in the /cgi-bin/tools/ajax_cmd endpoint of Panabit PAP-XM320 up to and including v7.7. The CGI component allows authenticated users to execute arbitrary shell commands with root privileges via the action=runcmd parameter.	8.8	More Details
CVE-2026-8526	Out of bounds write in WebRTC in Google Chrome prior to 148.0.7778.168 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-2026-45229	Quark Drive before 0.8.5 contains a mass assignment vulnerability in the POST /update endpoint that allows authenticated attackers to overwrite administrator credentials by posting an arbitrary webui object to the config_data dictionary. Attackers can exploit insufficient deny-list filtering to permanently replace stored login credentials, lock out legitimate administrators, and gain persistent access to all configured tasks, cloud tokens, and notification services.	8.8	More Details
CVE-2026-8522	Use after free in Downloads in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-8719	The AI Engine – The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to Privilege Escalation in version 3.4.9. This is due to missing WordPress capability enforcement in the MCP OAuth bearer-token authorization path, where any valid OAuth token causes MCP access to be granted without verifying administrator privileges. This makes it possible for authenticated (Subscriber+) attackers to invoke admin-level MCP tools and escalate privileges to Administrator.	8.8	More Details
CVE-2021-47979	WordPress Plugin Backup and Restore 1.0.3 contains an arbitrary file deletion vulnerability that allows authenticated attackers to delete files by manipulating parameters in AJAX requests. Attackers can send POST requests to admin-ajax.php with crafted file_name and folder_name parameters to delete arbitrary files from the WordPress installation directory.	8.8	More Details
CVE-2021-47976	TextPattern CMS 4.9.0-dev contains a remote code execution vulnerability that allows authenticated attackers to upload arbitrary PHP files by exploiting the plugin upload functionality. Attackers can authenticate, retrieve a CSRF token from the plugin event page, and upload malicious PHP files to the textpattern/tmp/ directory for code execution.	8.8	More Details
CVE-2026-44447	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 16.9.0, some endpoints were vulnerable to SQL injection through specially crafted requests, which would allow a malicious actor to extract sensitive information. This vulnerability is fixed in 16.9.0.	8.8	More Details
CVE-2026-44446	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.104.3 and 16.14.0, some endpoints were vulnerable to SQL injection through specially crafted requests, which would allow a malicious actor to extract sensitive information. This vulnerability is fixed in 15.104.3 and 16.14.0.	8.8	More Details
CVE-2026-8540	Type Confusion in V8 in Google Chrome prior to 148.0.7778.168 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-2026-42406	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Certificate Manager role can modify configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-41953	A vulnerability exists in BIG-IP systems where a highly privileged, authenticated attacker with at least the Resource Administrator role can modify configuration objects resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-44295	protobufjs-cli is the command line add-on for protobuf.js. Prior to 1.2.1 and 2.0.2, pbjs static code generation could emit unsafe JavaScript identifiers derived from schema-controlled names. When generating static JavaScript from a crafted schema or JSON descriptor, certain namespace, enum, service, or derived full names could be written into the generated output without sufficient sanitization. This vulnerability is fixed in 1.2.1 and 2.0.2.	8.7	More Details
CVE-2026-7481	GitLab has remediated an issue in GitLab EE affecting all versions from 16.4 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with developer-role permissions to execute arbitrary JavaScript in other users' browsers due to improper input sanitization.	8.7	More Details
CVE-2026-7377	GitLab has remediated an issue in GitLab EE affecting all versions from 18.7 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that, in customizable analytics dashboards, could have allowed an authenticated user to execute arbitrary JavaScript in the context of other users' browsers due to improper input sanitization.	8.7	More Details

CVE-2026-6073	GitLab has remediated an issue in GitLab EE affecting all versions from 18.7 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to execute arbitrary JavaScript in other users' browsers due to improper input sanitization.	8.7	More Details
CVE-2026-34176	When running in Appliance mode, an authenticated remote command injection vulnerability exists in an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-6346	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to sanitize sensitive configuration fields before including them in support packet generation, which allows a Mattermost System Admin or any party with access to a support packet to obtain sensitive credentials in plaintext via downloading a support packet from the System Console.. Mattermost Advisory ID: MMSA-2026-00607	8.7	More Details
CVE-2026-32673	A vulnerability exists in BIG-IP scripted monitors that may allow an authenticated attacker with the Resource Administrator or Administrator role to execute arbitrary system commands with higher privileges. In appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-44552	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the tool_servers and terminal_servers keys in utils/tools.py do use a prefix. When two or more Open WebUI instances share a Redis database (a supported and documented deployment pattern, e.g., for multi-region deployments, blue-green setups, or cluster topologies), the unprefixed keys collide. An admin on Instance A writing to tool_servers overwrites the value read by Instance B — causing Instance B's users to receive Instance A's tool server configuration. This vulnerability is fixed in 0.9.0.	8.7	More Details
CVE-2026-32643	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Certificate Manager role can modify configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-27173	JWT tokens that were used by workers in Kubernetes Executors have been exposed to users who had read only access to Kuberentes Pods. This could allow users with just read-only access to perform actions that were only available to running tasks via Task SDK and potentially allow to modify state of Airflow Database for tasks.	8.7	More Details
CVE-2026-40061	When BIG-IP DNS is provisioned, a vulnerability exists in an undisclosed iControl REST and BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with the Resource Administrator or Administrator role to execute arbitrary system commands with higher privileges. In Appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-33583	Exposure of the QKEY (used as input into the ‘OTA-Quantum’ device registration process) and internal system keys via an unauthenticated and unencrypted HTTP GET method in the Arqit Symmetric Key Agreement Platform. This issue affects Symmetric Key Agreement Platform: before 26.03.	8.7	More Details
CVE-2026-42924	An authenticated attacker with the Resource Administrator or Administrator role can create SNMP configuration objects through iControl SOAP resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-40698	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Resource Administrator role can create SNMP configuration objects through iControl REST or the TMOS shell (tmsh) resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-42930	When running in Appliance mode, an authenticated attacker assigned the 'Administrator' role may be able to bypass Appliance mode restrictions on a BIG-IP system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-40631	An authenticated attacker with the Resource Administrator or Administrator role can modify configuration objects through iControl SOAP resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2026-34241	CtrlPanel is open-source billing software for hosting providers. Versions 1.1.1 and prior contain a Stored Cross-Site Scripting (XSS) vulnerability in the ticket reply notification system. Unsanitized reply content ($newmessage) is stored directly in database notification payloads and later rendered unescaped via Blade's {!! !!} syntax in the recipient's browser. The flaw exists in both App\Notifications\Ticket\Admin\AdminReplyNotification (triggered when a user replies, targeting admins) and App\Notifications\Ticket\User\ReplyNotification (triggered when an admin replies, targeting users), allowing arbitrary JavaScript execution in the victim's session context. A low-privileged attacker can exploit this to hijack admin sessions, harvest credentials via fake login prompts or keyloggers, and escalate privileges by performing administrative actions on the victim's behalf. The reverse path also enables a malicious or compromised admin to target regular users in the same manner. This issue has been fixed in version 1.2.0.	8.7	More Details
CVE-2026-45315	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, the audio transcription upload endpoint takes the file extension from the user-supplied filename and saves the file under CACHE_DIR/audio/transcriptions/.. The /cache/{path} route serves these files via FileResponse, which sets Content-Type from the on-disk extension and emits no Content-Disposition. A verified user with the default-on chat.stt permission can upload a polyglot WAV+HTML file named pwn.html and trick any other user into opening the resulting URL — the response comes back as text/html and any embedded <script> runs in the Open WebUI origin. This vulnerability is fixed in 0.9.3.	8.7	More Details
CVE-2026-44001	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, a sandbox escape vulnerability in vm2 v3.10.5 allows any sandboxed code to crash the host Node.js process via a single Promise constructor that triggers an unhandled rejection propagating to the host. The fix for CVE-2026-22709 (v3.10.2) only sanitized the onRejected callback in .then() and .catch() overrides and did not address the executor-to-unhandledRejection path. This vulnerability is fixed in 3.11.0.	8.6	More Details
CVE-2026-20224	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to read arbitrary files that are stored in an affected system. The attacker does not need to have valid user credentials. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing an XML file. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to read arbitrary files that are stored in the affected system.	8.6	More Details
	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, Gotenberg's Chromium URL-to-PDF endpoint (/forms/chromium/convert/url) has no default protection against HTTP/HTTPS-based SSRF. The default deny-list regex only blocks file://		

CVE-2026-42595	URIs. An unauthenticated attacker can point Chromium at any internal IP — including loopback, RFC 1918 ranges, and cloud metadata endpoints — and receive the response rendered as a PDF. Additionally, even when operators configure a custom deny-list, the protection is bypassed via HTTP redirects. Gotenberg's Chromium instance follows 302 redirects from an attacker-controlled external URL to internal targets without re-validating the redirect destination against the deny-list. This vulnerability is fixed in 8.32.0.	8.6	More Details
CVE-2026-8958	Information disclosure, sandbox escape in the Security: Process Sandboxing component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	8.6	More Details
CVE-2026-29205	Incorrect privileges management and insufficient path filtering allow to read arbitrary file on the server via the cpdavd attachment download endpoints.	8.6	More Details
CVE-2026-6379	The WP Photo Album Plus WordPress plugin before 9.1.11.001 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-44578	Next.js is a React framework for building full-stack web applications. From 13.4.13 to before 15.5.16 and 16.2.5, self-hosted applications using the built-in Node.js server can be vulnerable to server-side request forgery through crafted WebSocket upgrade requests. An attacker can cause the server to proxy requests to arbitrary internal or external destinations, which may expose internal services or cloud metadata endpoints. Vercel-hosted deployments are not affected. This vulnerability is fixed in 15.5.16 and 16.2.5.	8.6	More Details
CVE-2026-45331	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, validate_url() in backend/open_webui/retrieval/web/utils.py calls validators.ipv6(ip, private=True), but the validators library does NOT implement the private keyword for IPv6 — the call raises a ValidationError (which is falsy in a boolean context), so every IPv6 address passes the filter. In addition, IPv4-mapped IPv6 (::ffff:10.0.0.1) bypasses the IPv4 check entirely, and several reserved IPv4 ranges (0.0.0.0/8, 100.64.0.0/10, 192.0.0.0/24, etc.) are not blocked. This vulnerability is fixed in 0.9.0.	8.5	More Details
CVE-2026-45400	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, a parsing difference between the urlparse and requests libraries led to an SSRF bypass vulnerability. This vulnerability is fixed in 0.9.5.	8.5	More Details
CVE-2026-45401	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, the validate_url() function in backend/open_webui/retrieval/web/utils.py only validates the initial URL submitted by the caller. The HTTP clients used downstream (sync requests, async aiohttp, langchain's WebBaseLoader) follow HTTP 3xx redirects by default and do not re-validate the redirect target against the private-IP / metadata-IP block list. Any authenticated user can therefore submit a public URL that 302-redirects to an internal address (e.g. 127.0.0.1, 169.254.169.254, RFC1918) and read the internal response body via the /api/v1/retrieval/process/web endpoint, the /api/v1/images/... endpoints, the /api/chat/completions endpoint with an image_url content part, and any other route that calls these helpers. This vulnerability is fixed in 0.9.5.	8.5	More Details
CVE-2026-43998	vm2 is an open source vm/sandbox for Node.js. In 3.10.5, NodeVM's require.root path restriction can be bypassed using filesystem symlinks, allowing sandboxed code to load modules from outside the allowed root directory in host context. Because path validation uses path.resolve() (which does not dereference symlinks) but module loading uses Node's native require() (which does), an attacker can load arbitrary host-realm modules and achieve remote code execution. This vulnerability is fixed in 3.11.0.	8.5	More Details
CVE-2020-37221	Atomic Alarm Clock 6.3 contains a stack overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string to the display name textbox in the Time Zones Clock configuration. Attackers can craft a buffer with structured exception handling overwrite and encoded shellcode to bypass SafeSEH protections and execute arbitrary commands with application privileges.	8.4	More Details
CVE-2026-5804	An improper authentication vulnerability was discovered in the Motorola Factory Test component (com.motorola.motocit). The application contained a reference to a writable file descriptor in external storage which could be used by third party apps running on the device to open a TCP server, exposing sensitive permissions and data. This could allow a local attacker to bypass permission checks and access protected device settings.	8.4	More Details
CVE-2026-41964	Permission control vulnerability in the web. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2026-25781	in OpenHarmony v6.0 and prior versions allow a local attacker cause DOS and it cannot be recovered.	8.4	More Details
CVE-2018-25322	Allok Fast AVI MPEG Splitter 1.2 contains a stack based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious license name string. Attackers can craft a payload with 780 bytes of junk data followed by structured shellcode and place it in the License Name field to trigger the overflow and execute code with application privileges.	8.4	More Details
CVE-2018-25328	VX Search 10.6.18 contains a local buffer overflow vulnerability that allows attackers to overwrite the instruction pointer by supplying an oversized string in the directory field. Attackers can craft a malicious input file containing 271 bytes of junk data followed by a return address to execute arbitrary code with application privileges.	8.4	More Details
CVE-2018-25323	Allok AVI DivX MPEG to DVD Converter 2.6.1217 contains a structured exception handler buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious payload. Attackers can craft a text file with a specially crafted buffer containing shellcode and SEH chain overwrite values, then paste the contents into the License Name field to trigger code execution.	8.4	More Details
CVE-2026-25705	A vulnerability has been identified in [Rancher's Extensions](https://ranchermanager.docs.rancher.com/integrations-in-rancher/rancher-extensions) where malicious code can be injected in Rancher through a path traversal in the `compressedEndpoint` field inside a `UIPlugin` deployment. A malicious UI extension could abuse that to: * Overwrite Rancher binaries or configuration to inject code. * Write to /var/lib/rancher/ to tamper with cluster state. * If hostPath volumes are mounted, write to the host node filesystem. * Use this issue to chain with other attack vectors.	8.4	More Details
CVE-2026-21821	The HCL BigFix SCM Reporting site contains an outdated and unsupported version of the jQuery 1.x library. Since jQuery 1.x has reached end-of-life and no longer receives security updates, it may expose the application to publicly known security weaknesses and increase the risk of client-side attacks such as Cross-Site Scripting (XSS) or manipulation through vulnerable third-party components.	8.3	More Details
CVE-	Use after free in FileSystem in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in		More

2026-8512	specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	Details
CVE-2026-8520	Race in Payments in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-32993	Improper sanitization of the `status` query parameter of the `/unprotected/nova_error` endpoint allows unauthenticated attacker to inject arbitrary HTTP header to the response.	8.3	More Details
CVE-2026-8513	Use after free in Input in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-44586	SiYuan is an open-source personal knowledge management system. From 2.1.12 to before 3.7.0. SiYuan's Bazaar marketplace renders package author metadata from the public bazaar stage feed into HTML without escaping. In the desktop app this becomes stored XSS, and because SiYuan's Electron windows are created with nodeIntegration: true and contextIsolation: false, a successful payload can call Node.js APIs and execute code on the host. This vulnerability is fixed in 3.7.0.	8.3	More Details
CVE-2026-43907	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, a signed integer overflow in QueryRGBBufferSizeInternal() in DPXColorConverter.cpp leads to a heap-based out-of-bounds write when processing crafted DPX image files. The function computes buffer sizes using 32-bit signed integer arithmetic with negative multipliers (e.g., pixels * -3 * bytes for kCbYCr descriptors and pixels * -4 * bytes for kABGR descriptors), where a negative result is used as an in-band signal that no separate buffer is needed. When the pixel count is sufficiently large, the multiplication overflows INT_MIN and wraps to a small positive value. The caller in dpxinput.cpp interprets this positive value as a required buffer size, allocates an undersized heap buffer via m_decodebuf.resize(), and then writes the full image data into it via fread, resulting in a heap buffer overflow. An attacker can exploit this by crafting a DPX file that triggers the overflow, causing a denial of service (crash) or potentially arbitrary code execution through heap corruption in any application that reads pixel data using OpenImageIO. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	8.3	More Details
CVE-2026-8515	Use after free in HID in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-8514	Use after free in Aura in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-8523	Use after free in Mojo in Google Chrome prior to 148.0.7778.168 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)	8.3	More Details
CVE-2026-8542	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.168 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)	8.3	More Details
CVE-2026-8525	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-8571	Insufficient policy enforcement in GPU in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-8530	Use after free in Network in Google Chrome on Windows prior to 148.0.7778.168 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)	8.3	More Details
CVE-2026-45369	python-utcp is the python implementation of UTCP. Prior to 1.1.3, the _substitute_utcp_args method in cli_communication_protocol.py inserts user-controlled tool_args values directly into shell command strings without any sanitization or escaping. These commands are then executed via /bin/bash -c (Unix) or powershell.exe -Command (Windows), allowing an attacker to inject arbitrary shell commands. This vulnerability is fixed in 1.1.3.	8.3	More Details
CVE-2026-8575	Use after free in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-8574	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-8573	Integer overflow in Codecs in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-44570	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.19, authorization controls surrounding the memories API were inconsistent, resulting in the ability of a standard user to delete, restore, and view the contents of other users' memories. Using a newly created non-admin user with no existing memories, it is possible to view existing memories via POST /api/v1/memories/query. Similarly, even if a non-admin user cannot modify another user's memory data via POST /api/v1/memories/{memory_id}/update, the endpoint's response improperly leaks the content of that memory if a valid memory_id is known. The DELETE /api/v1/memories/{memory_id} can also be used by any user to delete an existing memory. Deleted memories can then be restored by calling the POST /api/v1/memories/{memory_id}/update endpoint again. This vulnerability is fixed in 0.6.19.	8.3	More Details
CVE-2026-8569	Out of bounds write in Codecs in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	8.3	More Details

CVE-2026-8548	Out of bounds write in Media in Google Chrome prior to 148.0.7778.168 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)	8.3	More Details
CVE-2026-8533	Use after free in Accessibility in Google Chrome prior to 148.0.7778.168 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)	8.3	More Details
CVE-2026-8534	Integer overflow in GPU in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 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)	8.3	More Details
CVE-2020-37243	Supsystic Pricing Table 1.8.7 contains an SQL injection vulnerability in the 'sidx' GET parameter that allows unauthenticated attackers to execute arbitrary SQL queries through the getListForTbl action. The plugin also contains stored cross-site scripting vulnerabilities in the 'Edit name' and 'Edit HTML' fields that execute malicious scripts when viewing pricing tables.	8.2	More Details
CVE-2021-47956	EgavilanMedia PHPCRUD 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the firstname parameter. Attackers can send POST requests to insert.php with malicious firstname values to extract sensitive database information.	8.2	More Details
CVE-2021-47954	LayerBB 1.1.4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the search_query parameter. Attackers can send POST requests to /search.php with malicious search_query values using CASE WHEN statements to extract sensitive database information.	8.2	More Details
CVE-2021-47966	PHP Timeclock 1.04 contains time-based and boolean-based blind SQL injection vulnerabilities in the login_userid parameter of login.php that allows unauthenticated attackers to extract database contents. Attackers can submit crafted POST requests with SQL payloads using SLEEP functions or RLIKE conditional statements to dump sensitive database information including employee names and credentials.	8.2	More Details
CVE-2026-5396	The Fluent Forms plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to, and including, 6.1.21. This is due to the SubmissionPolicy class authorizing submission-level actions (read, modify, delete, add notes) based on a user-supplied `form_id` query parameter. This makes it possible for authenticated attackers, with Fluent Forms Manager access restricted to specific forms, to read, modify status, add notes to, and permanently delete form submissions belonging to any other form by spoofing the form_id parameter to a form they are authorized for.	8.2	More Details
CVE-2020-37244	Supsystic Membership 1.4.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'search' and 'sidx' parameters. Attackers can send GET requests to the badges module with crafted payloads to extract sensitive database information using time-based blind or UNION-based SQL injection techniques.	8.2	More Details
CVE-2026-46720	Net::Statsd::Tiny versions before 0.3.8 for Perl allowed metric injections. The metric names and set values were not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics.	8.2	More Details
CVE-2020-37242	Supsystic Ultimate Maps 1.1.12 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'sidx' GET parameter. Attackers can send crafted requests to the getListForTbl action with boolean-based blind or time-based blind SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2026-46728	Das U-Boot before 2026.04 allows FIT (Flat Image Tree) signature verification bypass because hashed-nodes is omitted from a hash.	8.2	More Details
CVE-2026-42590	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.30.0, The ExifTool metadata write blocklist in Gotenberg can be bypassed using ExifTool's group-prefix syntax, enabling arbitrary file rename, move, hardlink, and symlink creation on the server. ExifTool supports group-prefix syntax where File:FileName is processed identically to FileName -- the prefix is stripped by SetNewValue in Writer.pl before tag matching. The safeKeyPattern regex (^[a-zA-Z0-9\-_.:]+$) allows colons, so prefixed tag names pass validation. Any prefix works: File:FileName, System:Directory, a:HardLink, etc. Additionally, FilePermissions, FileUserID, and FileGroupID pseudo-tags are not blocked at all and can modify file attributes without any prefix. This vulnerability is fixed in 8.30.0.	8.2	More Details
CVE-2026-5395	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.2.0 via the exportEntries function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Fluent Forms manager-level access and above, to bypass form-level access restrictions to access submissions from forms they are not authorized to view, export data from arbitrary database tables, and enumerate database table names via error message disclosure.	8.2	More Details
CVE-2026-40893	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, Gotenberg only checks if the tag is exactly FileName, so System:FileName slips right through and ExifTool happily renames the file. This allows remote attackers to move, rename, and change permissions for arbitrary files. This vulnerability is fixed in 8.31.0.	8.2	More Details
CVE-2026-8657	Versions of the package jsondiffpatch before 0.7.6 are vulnerable to Prototype Pollution via the jsondiffpatch.patch() and jsondiffpatch/formatters/jsonpatch.patch() APIs. An attacker can perform prototype pollution by supplying crafted delta or JSON Patch documents, as attacker-controlled property names and path segments are used to traverse and modify objects without restricting access to special properties like __proto__ or constructor.prototype, allowing modification of Object.prototype.	8.2	More Details
CVE-2026-42591	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, the LibreOffice conversion endpoint (/forms/libreoffice/convert) passes uploaded documents directly to LibreOffice without inspecting their content. LibreOffice then fetches any embedded external URLs on its own, completely bypassing the SSRF filters. This vulnerability is fixed in 8.32.0.	8.2	More Details
CVE-2026-32992	SSL verification is disabled in the DNS Cluster system. This could allow for a malicious server to man-in-the-middle the request and capture credentials.	8.2	More Details
CVE-2018-25339	Zechat 1.5 contains a SQL injection vulnerability in the v parameter that allows unauthenticated attackers to extract database information using time-based blind techniques. Attackers can exploit the v parameter with sleep-based blind injection to confirm vulnerability and extract data.	8.2	More Details
CVE-	A buffer underflow vulnerability has been identified in the ogg123 utility from the vorbis-tools 1.4.3 package in function remotethread in		More

2026-34253	remote.c. This vulnerability occurs in the remote control functionality when processing malformed input, leading to a stack buffer underflow that can cause application crashes and potentially allow code execution.	8.2	Details
CVE-2026-22810	Joplin is an open source note-taking and to-do application that organises notes and lists into notebooks. Versions prior to 3.5.7 contain a path traversal vulnerability in the importer which allows overwriting arbitrary files on disk. The OneNote converter does not sanitize the names of embedded files before writing them to disk. As a result, it's possible for an attacker to create a malicious .one file that includes file names containing ../../, that are then interpreted as part of the target path when extracting attachments from the .one file. This issue has been patched in version 3.5.7.	8.2	More Details
CVE-2018-25330	Joomla! extension EkRishta 2.10 contains persistent cross-site scripting and SQL injection vulnerabilities that allow attackers to inject malicious code through profile fields and POST parameters. Attackers can inject script payloads in profile information fields like Address that execute when users visit the profile, or submit SQL injection payloads via the phone_no parameter to the user_setting endpoint to manipulate database queries.	8.2	More Details
CVE-2018-25333	Nordex N149/4.0-4.5 Wind Turbine Web Server 4.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the login parameter in login.php. Attackers can submit crafted POST requests with SQL injection payloads in the login field to extract sensitive database information and bypass authentication mechanisms.	8.2	More Details
CVE-2020-37218	Joomla com_hdwplayer 4.2 contains an SQL injection vulnerability in the search.php file that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the hdwplayersearch parameter. Attackers can submit POST requests with crafted SQL payloads in the hdwplayersearch parameter to extract sensitive database information from the hdwplayer_videos table.	8.2	More Details
CVE-2018-25338	Zechat 1.5 contains a SQL injection vulnerability in the hashtag parameter that allows unauthenticated attackers to extract database information using union-based techniques. Attackers can exploit the hashtag parameter with union-based payloads to retrieve table and column names.	8.2	More Details
CVE-2026-7635	The coreActivity: Activity Logging for WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.0. This is due to the plugin failing to validate or strip PHP serialization syntax from the User-Agent HTTP header before storing it in the logmeta table, and subsequently calling `maybe_unserialize()` on every retrieved `meta_value` in `query_metas()` without verifying the data was originally serialized by the application. This makes it possible for unauthenticated attackers to inject a crafted PHP serialized payload via the User-Agent header during any logged event (such as a failed login attempt), which, when an administrator views the Logs page, is deserialized and passed to `DeviceDetector::setUserAgent()`, triggering a Fatal TypeError that creates a persistent Denial of Service condition blocking administrator access to the Logs page entirely.	8.1	More Details
CVE-2026-8711	NGINX JavaScript has a vulnerability when the js_fetch_proxy directive is configured with at least one client-controlled NGINX variable (for example, $http_*, $arg_*, $cookie_*) and a location invoking the ngx.fetch() operation from NGINX JavaScript. An unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-44574	Next.js is a React framework for building full-stack web applications. From 15.4.0 to before 15.5.16 and 16.2.5, applications that rely on middleware to protect dynamic routes can be vulnerable to authorization bypass. In affected deployments, specially crafted query parameters can alter the dynamic route value seen by the page while leaving the visible path unchanged, which can allow protected content to be rendered without passing the expected middleware check. This vulnerability is fixed in 15.5.16 and 16.2.5.	8.1	More Details
CVE-2026-4030	The Database Backup for WordPress plugin for WordPress is vulnerable to unauthorized arbitrary file read and deletion in all versions up to, and including, 2.5.2. This is due to the plugin not properly enforcing the return value of its authorization check combined with a user-controlled backup directory parameter. This makes it possible for unauthenticated attackers to read and delete arbitrary files on the server, leading to Sensitive Information Exposure and potential site takeover. Note: This vulnerability is only exploitable in WordPress Multisite environments where the deprecated is_site_admin() function exists.	8.1	More Details
CVE-2026-44291	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs used plain objects with inherited prototypes for internal type lookup tables used by generated encode and decode functions. If Object.prototype had already been polluted, those lookup tables could resolve attacker-controlled inherited properties as valid protobuf type information. This could cause attacker-controlled strings to be emitted into generated JavaScript code. This vulnerability is fixed in 7.5.6 and 8.0.2.	8.1	More Details
CVE-2026-3892	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 1.4.107. This is due to insufficient file path validation in the become-dealer logo upload flow. The plugin allows any authenticated user to set an arbitrary filesystem path via the profile update handler. This makes it possible for authenticated attackers, with subscriber level access and above, to delete arbitrary files on the server.	8.1	More Details
CVE-2026-42463	SQLBot is an intelligent Text-to-SQL system based on large language models and RAG. Prior to 1.8.0, SQLBot contains a Cross-Workspace IDOR (Insecure Direct Object Reference) and Authorization Bypass vulnerability in the /api/v1/datasource/exportDsSchema and /api/v1/datasource/uploadDsSchema endpoints. An attacker can access and modify database schemas and data sources belonging to other tenants/workspaces. This vulnerability is fixed in 1.8.0.	8.1	More Details
CVE-2026-8969	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	8.1	More Details
CVE-2026-6282	A potential improper file path validation vulnerability was reported in some Lenovo Personal Cloud Storage devices that could allow a remote authenticated user to move or access files belonging to other users on the same device.	8.1	More Details
CVE-2026-42602	azureauthextension is the Azure Authenticator Extension. From 0.124.0 to 0.150.0, a server-side authentication bypass in azureauthextension allows any party who holds a single valid Azure access token for any scope the collector's configured identity can mint for to authenticate to any OpenTelemetry receiver that uses auth: azure_auth. The extension's Authenticate method does not validate incoming bearer tokens as JWTs. Instead, it calls its own configured credential to obtain an access token and compares the client's token to the result with string equality — and the scope for that server-side token request is taken from the client-supplied Host header. As a result, a token minted for any Azure resource the service principal has ever been issued a token for (ARM, Graph, Key Vault, Storage, etc.) will authenticate to the collector if the attacker picks a matching Host. Tokens are replayable for the full issued lifetime (commonly several hours for managed identity tokens).	8.1	More Details
CVE-2026-29206	Insufficient sanitization of SQL queries in the `sqloptimizer` utility script allows SQL Injections on behalf of the root user if Slow Query logging is enabled.	8.1	More Details

CVE-2026-45665	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Banner component due to an improper sanitization order (specifically, DOMPurify is executed before the marked library). This vulnerability allows a compromised or malicious administrator to plant a malicious payload in the global banner. Crucially, this vector enables Privilege Escalation, as the malicious banner is rendered for all users, including the Super Admin (Primary Admin). Consequently, the payload successfully bypasses the existing security mechanism. An attacker can leverage this to steal the Super Admin's session token This vulnerability is fixed in 0.8.0.	8.1	More Details
CVE-2026-45055	CubeCart is an ecommerce software solution. Prior to 6.7.2, CubeCart 6.6.x – 6.7.1 builds CC_STORE_URL directly from the Host request header at bootstrap, with no allowlist. The constant is embedded verbatim into transactional email links, most critically the password-reset link in User::passwordRequest() (and the admin equivalent in Admin::passwordRequest()). An unauthenticated attacker who knows a target email can POST /index.php?_a=recover with Host: evil.com; CubeCart writes a fresh verify token (valid 3,600 s) and emails the victim a link http://evil.com/index.php?_a=recovery&validate=<TOKEN>. The token is valid against the legitimate store — capturing the victim's click on evil.com yields full account takeover, or store takeover when an admin email is targeted. This vulnerability is fixed in 6.7.2.	8.1	More Details
CVE-2026-45402	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, multiple endpoints accept a user-supplied file_id and attach the referenced file to a resource the caller controls (folder knowledge, knowledge-base contents) without verifying that the caller owns or has been granted access to the file. The file's content then becomes reachable through the downstream RAG / file-content paths, allowing any authenticated user to exfiltrate any other user's private file — and on the knowledge-base path, also to overwrite it — given knowledge of the file's UUID. This affects backend/open_webui/routers/folders.py (POST /api/v1/folders/{id}/update), backend/open_webui/routers/knowledge.py (add_file_to_knowledge_by_id), and backend/open_webui/routers/knowledge.py (add_files_to_knowledge_by_id_batch). This vulnerability is fixed in 0.9.5.	8.1	More Details
CVE-2026-45301	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.3.16, a missing permission check in all files related API endpoints allows any authenticated user to list, access and delete every file uploaded by every user to the platform. This vulnerability is fixed in 0.3.16.	8.1	More Details
CVE-2026-42945	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-20916	An authenticated iControl REST user with low privileges can create or modify arbitrary files through an undisclosed iControl REST endpoint on the BIG-IQ system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-8629	Crabbox prior to v0.12.0 contains a privilege escalation vulnerability that allows users with shared visibility-only access to obtain Code, WebVNC, and Egress agent tickets by sending POST requests to ticket endpoints. Attackers can exploit insufficient access control checks on the /v1/leases/:id/code/ticket, /v1/leases/:id/webvnc/ticket, and /v1/leases/:id/egress/ticket endpoints to obtain bridge-agent tickets and impersonate trusted lease-side bridges despite having only visibility permissions.	8.1	More Details
CVE-2026-4094	The FOX – Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the 'admin_head' function in all versions up to, and including, 1.4.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete the entire multi-currency configuration by visiting any wp-admin page with the `woocs_reset` parameter appended. Additionally, because no nonce is verified, this is also exploitable via Cross-Site Request Forgery against any administrator. The vulnerability may also be exploited by Subscriber-level users if the site is configured to allow Subscriber access to 'wp-admin' pages.	8.1	More Details
CVE-2026-7504	A flaw was found in Keycloak's URL validation logic during redirect operations. By crafting a malicious request, an attacker could bypass validation to redirect users to unauthorized URLs, potentially leading to the exposure of sensitive information within the domain or facilitating further attacks. This vulnerability specifically affects Keycloak clients configured with a wildcard (*) in the "Valid Redirect URIs" field and requires user interaction to be successfully exploited. The issue stems from a discrepancy in how Keycloak and the underlying Java URI implementation handle the user-info component of a URL. If a malicious redirect URL is constructed using multiple @ characters in the user-info section, Java's URI parser fails to extract the user-info, leaving only the raw authority field. Consequently, Keycloak's validation check fails to detect the malformed user-info, falls back to a wildcard comparison, and incorrectly permits the malicious redirect.	8.1	More Details
CVE-2026-44633	Live Helper Chat is an open-source application that enables live support websites. In 4.84v, the Live Helper Chat REST API chat update endpoint allows a REST user with lhchat/use to update a chat in a department they cannot read. The endpoint accepts arbitrary chat object fields, so the user can change the chat hash and status and then access or tamper with the chat through visitor/widget paths. The same write primitive can set operation_admin, which is later emitted as operator-side JavaScript.	8.1	More Details
CVE-2026-35194	Code injection in SQL code generation in Apache Flink 1.15.0 through 1.20.x and 2.0.0 through 2.x allows authenticated users with query submission privileges to execute arbitrary code on TaskManagers via maliciously crafted SQL queries. The vulnerability affects JSON functions (1.15.0+) and LIKE expressions with ESCAPE clauses (1.17.0+). User-controlled strings are interpolated into generated Java code without proper escaping, allowing attackers to break out of string literals and inject arbitrary expressions. Users are recommended to upgrade to either version 1.20.4, 2.0.2, 2.1.2 or 2.2.1, which fixes this issue.	8.1	More Details
CVE-2026-44565	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.10, when uploading an audio file, the name of the file is derived from the original HTTP upload request and is not validated or sanitized. This allows for users to upload files with names containing dot-segments in the file path and traverse out of the intended uploads directory. Effectively, users can upload files anywhere on the filesystem the user running the web server has permission. This vulnerability is fixed in 0.6.10.	8.1	More Details
CVE-2026-42897	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-2026-24792	in OpenHarmony v6.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps.	8.1	More Details
	CtrlPanel is open-source billing software for hosting providers. Versions 1.1.1 and prior contains a broken access control vulnerability where multiple admin controllers enforce permission checks on form display methods but omit equivalent checks on the corresponding write methods, allowing any authenticated user to bypass RBAC via direct POST/PATCH requests. Controllers missing checks on write		

CVE-2026-34358	methods store() and update() include ApplicationApiController (admin.api.write), CouponController (admin.coupons.write), PartnerController (admin.partners.write), ShopProductController (admin.store.write), UsefulLinkController (admin.useful_links.write), and VoucherController (admin.voucher.write); ProductController (admin.products.edit), ServerController (write/change_owner/change_identifier), and UserController (write/change_email/change_credits/change_username/change_password/change_role/change_referral/change_ptero/change_serverlimit) are missing checks on update() only, and ActivityLogController exposed empty stub store()/update() methods that silently accepted any request. An authenticated attacker without admin write privileges can issue API credentials, generate unlimited coupons and vouchers, assign arbitrary partner commission and discount rates, alter shop product pricing and limits, reassign server ownership or identifiers, and modify user accounts including roles, credits, passwords, and linked Pterodactyl IDs to achieve full privilege escalation, as well as abuse logBackIn() without the login_as permission to interfere with admin impersonation sessions. This issue has been fixed in version 1.2.0.	8.1	More Details
CVE-2026-8851	SOGo versions 5.12.7 and prior contains a SQL injection vulnerability in the Access Control List management functionality that allows authenticated users to extract arbitrary data from the database by injecting SQL subqueries through the uid parameter of the addUserInAcls endpoint. Attackers can inject malicious SQL code to write extracted data into the sogo_acl table and retrieve it through the /acls API, establishing an out-of-band data exfiltration channel.	8.1	More Details
CVE-2026-46407	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.3, the backend admin/auth-token endpoint allows an authenticated administrator to load another administrator's REST API token list by supplying that user's admin_id. This can disclose sensitive API tokens belonging to other administrators. This vulnerability is fixed in 1.0.8.3.	8.1	More Details
CVE-2026-45675	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, he LDAP and OAuth authentication flows use a TOCTOU (Time-of-Check-Time-of-Use) pattern for first-user admin role assignment. The regular signup handler (signup_handler in auths.py, line 663) was explicitly patched to prevent this race with the comment "Insert with default role first to avoid TOCTOU race", but the LDAP and OAuth code paths were never updated with the same fix. This vulnerability is fixed in 0.9.0.	8.1	More Details
CVE-2026-44553	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, administrative role changes and user deletions do not iterate SESSION_POOL to disconnect affected sessions. As a result, a user whose admin role has been revoked retains admin privileges within their existing Socket.IO session for as long as they keep the connection alive (via automatic heartbeats). The gap is exclusive to the Socket.IO session cache. This vulnerability is fixed in 0.9.0.	8.1	More Details
CVE-2026-44554	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the POST /api/v1/retrieval/process/web endpoint accepts a user-supplied collection_name and an overwrite query parameter (default: True). It performs no authorization check on whether the calling user owns or has write access to the target collection. When overwrite=True, save_docs_to_vector_db calls VECTOR_DB_CLIENT.delete_collection() on the target collection before writing new content. This vulnerability is fixed in 0.9.0.	8.1	More Details
CVE-2026-45671	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, any authenticated user can permanently delete files owned by other users via DELETE /api/v1/files/{id} when the target file is referenced in any shared chat. The has_access_to_file() authorization gate unconditionally grants access through its shared-chat branch. It checks neither the requesting user's identity nor the type of operation being performed. File UUIDs (which would otherwise be impractical to guess) are disclosed to any user with read access to a knowledge base via GET /api/v1/knowledge/{id}/files. This vulnerability is fixed in 0.9.0.	8.0	More Details
CVE-2026-41217	A vulnerability exists in an undisclosed BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with resource administrator or administrator role to execute arbitrary system commands with higher privileges. In Appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.9	More Details
CVE-2026-41702	VMware Fusion contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during an operation performed by a SETUID binary. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed.	7.8	More Details
CVE-2026-47092	Claude HUD through 0.0.12, patched in commit 234d9aa, contains a command injection vulnerability that allows local attackers to execute arbitrary commands by manipulating the COMSPEC environment variable. Attackers can set COMSPEC to an arbitrary binary path before claude-hud performs its version check, causing execFile() to execute the attacker-supplied executable with cmd.exe arguments, resulting in arbitrary code execution on Windows systems.	7.8	More Details
CVE-2020-37229	OKI sPSV Port Manager 1.0.41 contains an unquoted service path vulnerability in the sPSVOpLclSrv service that allows local attackers to escalate privileges by inserting executable files into the unquoted path. Attackers can place a malicious executable in a directory within the service path that will execute with LocalSystem privileges when the service restarts or the system reboots.	7.8	More Details
CVE-2026-30905	External Control of File Name or Path in the Zoom Workplace VDI Plugin Windows Universal Installer before version 6.6.11 may allow an authenticated user to conduct an escalation of privilege via local access.	7.8	More Details
CVE-2026-30906	Untrusted search path in the installer for Zoom Rooms for Windows before version 7.0.0 may allow an authenticated user to enable an escalation of privilege via local access.	7.8	More Details
CVE-2026-47314	Out-of-bounds write vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	7.8	More Details
CVE-2026-47311	Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	7.8	More Details
CVE-2026-47310	Use after free vulnerability in Samsung Open Source Escargot allows Pointer Manipulation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	7.8	More Details
CVE-2024-36333	A DLL hijacking vulnerability in the AMD Cleanup Utility could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.8	More Details
CVE-	Syncplify.me Server! 5.0.37 contains an unquoted service path vulnerability in the SMWebRestServicev5 service that allows local		

2020-37230	attackers to escalate privileges by exploiting the unquoted binary path. Attackers can insert a malicious executable into the service path and execute it with LocalSystem privileges when the service restarts or the system reboots.	7.8	More Details
CVE-2026-43906	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, a heap-based buffer overflow in the HEIF decoder of OpenImageIO allows out-of-bounds writes via crafted images due to a subimage metadata mismatch, leading to memory corruption and potential code execution. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	7.8	More Details
CVE-2020-37247	Kite 4.2.0.1 U1 contains an unquoted service path vulnerability in the KiteService Windows service that allows local attackers to escalate privileges by exploiting the service binary path. Attackers can place a malicious executable in the Program Files directory to be executed with LocalSystem privileges when the service starts.	7.8	More Details
CVE-2026-43904	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, softimageinput.cpp:469 (mixed RLE) and :345 (pure RLE) do not clamp the run length to remaining scanline width before writing pixels. The raw packet path (line 403) correctly clamps with std::min, but RLE paths skip this check. A crafted .pic file causes heap overflow up to 65535 bytes. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	7.8	More Details
CVE-2026-43903	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, sgiinput.cpp:265,274 use OIIO_DASSERT for bounds checking in the RLE decode loop. In release builds, OIIO_DASSERT compiles to ((void)sizeof(x)) (dassert.h:210), making all bounds checks no-ops. A crafted .sgi file with RLE count exceeding scanline width causes heap buffer overflow and crash. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	7.8	More Details
CVE-2026-23558	The adjustments made for XSA-379 as well as those subsequently becoming XSA-387 still left a race window, when a HVM or PVH guest does a grant table version change from v2 to v1 in parallel with mapping the status page(s) via XENMEM_add_to_physmap. Some of the status pages may then be freed while mappings of them would still be inserted into the guest's secondary (P2M) page tables.	7.8	More Details
CVE-2020-37231	Privacy Drive 3.17.0 contains an unquoted service path vulnerability in the pdsvc.exe service binary that allows local attackers to escalate privileges by exploiting the service startup process. Attackers can place malicious executables in the unquoted path directories to execute arbitrary code with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2020-37232	Advanced System Care Service 13.0.0.157 contains an unquoted service path vulnerability in the AdvancedSystemCareService13 service binary path that allows local attackers to escalate privileges. Attackers can place malicious executables in the system root path that will be executed with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2026-46508	Turborepo is a high-performance build system for JavaScript and TypeScript codebases. Prior to 2.9.14000, the Turborepo LSP VS Code extension could execute shell commands derived from workspace-controlled values. The extension used string-based command execution for Turborepo daemon commands and task runs. A malicious workspace could provide crafted values through workspace settings or task names in the repository's source code that were interpolated into shell commands. When the extension activated or when a user ran a task through the extension, those values could be interpreted by the user's shell, allowing arbitrary command execution with the privileges of the local VS Code process. This vulnerability is fixed in 2.9.14000.	7.8	More Details
CVE-2026-44471	gitoxide is an implementation of git written in Rust. Prior to 0.21.1, a malicious tree can be constructed that will, when checked out with gitoxide, permit writing an attacker-controlled symlink into any existing directory the user has write access to. During checkout, all symlink index entries are deferred and created after regular files using a single shared gix_worktree::Stack. Internally, this uses a gix_fs::Stack. gix_fs::Stack::make_relative_path_current() caches validated path prefixes: when the previously-processed leaf component exactly matches the leading component(s) of the next path, the leaf-to-directory transition at gix-fs/src/stack.rs invokes only delegate.push_directory(), never delegate.push(). In gix_worktree::stack::delegate::StackDelegate, when the state member is State::CreateDirectoryAndAttributesStack, Attributes::push_directory() only loads attributes (from the ODB, in the clone case), and does not perform any other checks. The on-disk symlink_metadata() check and unlink-on-collision live in StackDelegate::push()'s invocation of create_leading_directory(), which is therefore bypassed for the cached prefix. The final symlink is created with plain std::os::unix::fs::symlink, which follows symlinks in parent directories. Therefore, it's possible to provide a tree with duplicate symlink and directory entries that exploits this. This vulnerability is fixed in 0.21.1.	7.8	More Details
CVE-2026-45038	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.233, since Tabby does not escape control characters from file paths when dragging and dropping a file into it, code execution can be achieved. This vulnerability is fixed in 1.0.233.	7.8	More Details
CVE-2021-47974	VX Search 13.5.28 contains an unquoted service path vulnerability in both VX Search Server and VX Search Enterprise services that allows local attackers to escalate privileges. Attackers can place malicious executables in unquoted path directories like C:\Program Files\VX Search to execute arbitrary code with LocalSystem privileges when services restart.	7.8	More Details
CVE-2026-43905	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, jpeg2000input.cpp:395 computes buffer size as const int bufsize = w * h * ch * buffer_bpp using signed 32-bit arithmetic. When the product exceeds INT_MAX, the result wraps to 0 or a small value. m_buf.resize() allocates an undersized buffer, and subsequent pixel write loops cause heap overflow. Conditional on USE_OPENJPH build flag. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	7.8	More Details
CVE-2026-21020	Improper export of android application components in OmaCP prior to SMR May-2026 Release 1 allows local attackers to trigger privileged functions.	7.8	More Details
CVE-2020-37223	IObit Uninstaller 9.5.0.15 contains an unquoted service path vulnerability in the IObitUnSvr service that allows local attackers to escalate privileges to SYSTEM level. Attackers can place a malicious executable named IObit.exe in the C:\Program Files (x86)\IObit directory and restart the service to execute code with SYSTEM privileges.	7.8	More Details
CVE-2026-42290	protobufjs-cli is the command line add-on for protobuf.js. Prior to 1.2.1 and 2.0.2, pbts invoked JSDoc by building a shell command string from input file paths and executing it through child_process.exec. File paths containing shell metacharacters could therefore be interpreted by the shell instead of being passed to JSDoc as plain arguments. This vulnerability is fixed in 1.2.1 and 2.0.2.	7.8	More Details
CVE-2026-45370	python-utcp is the python implementation of UTCP. Prior to 1.1.3, _prepare_environment() in cli_communication_protocol.py passes a full copy of os.environ to every CLI subprocess. When combined with CVE-2026-45369, an attacker can exfiltrate all process-level secrets in a single tool call. This vulnerability is fixed in 1.1.3.	7.7	More Details
CVE-	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.5, through the HTML rendering view, scripts can be injected and executed. The frontend provides a function to visualize the HTML content of a current chat.		

2026-45303	The content is embedded in an iFrame with the allow-scripts allow-forms allow-same-origin sandbox directive. This means that the content is placed in a sandbox but with permission to execute scripts and access the parent’s data (e.g., local storage). As a result, only a few functions are restricted (e.g., displaying an alert box), but in effect, the sandbox attribute is largely nullified. This vulnerability is fixed in 0.6.5.	7.7	More Details
CVE-2026-42283	DevSpace is a client-only developer tool for cloud-native development with Kubernetes. Prior to 6.3.21, DevSpace's UI server WebSocket accepts connections from all origins by default, and therefore several endpoints are exposed via this WebSocket. When a developer runs the DevSpace UI and at the same time uses a browser to access the internet, a malicious website they visit can use their browser to establish a cross-origin WebSocket connection to ws://127.0.0.1:8090. This vulnerability is fixed in 6.3.21.	7.7	More Details
CVE-2026-41948	Dify version 1.14.1 and prior contain a path traversal vulnerability that allows authenticated users to manipulate requests forwarded to the Plugin Daemon's internal REST API by exploiting insufficient URL path sanitization. Attackers can traverse out of their authorized tenant path using unencoded dot sequences in task identifiers or manipulated filename parameters to access internal endpoints such as debug interfaces, requiring only knowledge of the victim tenant's UUID. NOTE: Dify Cloud allows unauthenticated free self-registration, making account creation trivially accessible to any attacker.	7.7	More Details
CVE-2026-45338	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, a Server-Side Request Forgery (SSRF) vulnerability exists in _process_picture_url() in backend/open_webui/utils/oauth.py (line ~1338). The function fetches arbitrary URLs from OAuth picture claims without applying validate_url(), allowing an attacker to force the server to make HTTP requests to internal resources and exfiltrate the full response. This vulnerability is fixed in 0.9.0.	7.7	More Details
CVE-2026-6347	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to sanitize sensitive configuration fields in the Mattermost Calls plugin which allows an attacker with access to a support packet to obtain TURN server credentials via the plaintext values present in the exported plugin configuration.. Mattermost Advisory ID: MMSA-2026-00605	7.6	More Details
CVE-2026-44516	Valtimo is an open-source business process automation platform. From 12.4.0 to 12.33.0 and 13.26.0, the LoggingRestClientCustomizer in the web module automatically intercepts all outgoing HTTP calls made via Spring's RestClient and logs the full request body, response body, and response headers. When an error response is received, this information is included in the thrown HttpClientErrorException message, which is logged at ERROR level by Spring's default exception handling — regardless of the application's DEBUG log level setting. This vulnerability is fixed in 12.33.0 and 13.26.0.	7.6	More Details
CVE-2026-33233	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. In versions 0.6.34 through 0.6.51, the backend deserializes Redis cache bytes using pickle.loads without integrity/authenticity checks. The write path serializes values with pickle.dumps(...) into Redis and the read path blindly invokes pickle.loads(...) on bytes with no HMAC/signature or strict schema validation gating deserialization. If an attacker can poison a shared-cache key in Redis, arbitrary command execution is possible in the backend container context, affecting confidentiality, integrity, and availability. This issue has been fixed in version 0.6.52.	7.6	More Details
CVE-2026-44555	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, Open WebUI supports model composition via base_model_id: a user-defined model (e.g., "Cheap Assistant") can reference an existing base model (e.g., "gpt-4-turbo-restricted") that provides the actual inference capability. When a user queries the composed model, the access control pipeline verifies the user has access to the composed model but never re-verifies access to the chained base model. Additionally, the model creation and import endpoints accept arbitrary base_model_id values without checking that the caller has access to that base model. Combined, this allows any user with the default model creation permission to create a model that chains to a restricted base model — and then invoke it, causing the server to dispatch the request to the restricted base model using the admin-configured API key. This vulnerability is fixed in 0.9.0.	7.6	More Details
CVE-2026-46408	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.3, the checkout endpoint accepts a user-controlled cart_id and uses it to enter the payment flow without verifying cart ownership. A logged-in attacker can therefore reuse another user's cart data in their own checkout session. This vulnerability is fixed in 1.0.8.3.	7.6	More Details
CVE-2026-46367	phpMyFAQ before 4.1.2 contains a stored cross-site scripting vulnerability in Utils::parseUrl() that allows authenticated users to inject JavaScript via malformed URLs in comments. Attackers can craft URLs with unescaped quotes to inject event handlers, stealing admin session cookies and achieving full application takeover when visitors view affected FAQ pages.	7.6	More Details
CVE-2026-33633	Kitty is a cross-platform GPU based terminal. Versions 0.46.2 and below contain a heap buffer overflow in load_image_data() that allows any process which can write to the terminal's stdin to crash kitty immediately. The vulnerability is triggered by a single APC graphics protocol command with a PNG format declaration (f=100) whose payload exceeds twice the initial buffer capacity. The overflow is attacker-controlled in both length and content, causing DoS and potentially escalation to RCE itself. This issue has been fixed in version 0.47.0.	7.5	More Details
CVE-2026-44673	libyang is a YANG data modeling language library. Prior to SO 5.2.15, lyb_read_string() in src/parser_lyb.c contains an integer overflow that results in a heap buffer overflow when parsing a maliciously crafted LYB binary blob. An attacker who can supply LYB data to any libyang consumer (NETCONF server, sysrepo, etc.) can trigger a crash or potential heap corruption. This vulnerability is fixed in SO 5.2.15.	7.5	More Details
CVE-2020-37245	Supsystic Digital Publications 1.6.9 contains a path traversal vulnerability in the Folder input field that allows attackers to access files outside the web root by injecting directory traversal sequences. Additionally, the plugin fails to sanitize input fields in publication settings, allowing stored cross-site scripting attacks through script injection in parameters like Area Width and Publication Width that execute when publications are viewed or edited.	7.5	More Details
CVE-2026-6929	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'sortf' parameter in all versions up to, and including, 5.7.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2026-1659	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.0 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to cause denial of service by sending specially crafted requests due to insufficient input validation.	7.5	More Details
CVE-2026-8585	Inappropriate implementation in Media in Google Chrome on iOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs allowed certain schema option paths to traverse through inherited object properties while applying options. A crafted protobuf schema or JSON descriptor could cause		More

2026-44290	option handling to write to properties on global JavaScript constructors, corrupting process-wide built-in functionality. This vulnerability is fixed in 7.5.6 and 8.0.2.	7.5	Details
CVE-2026-44671	ZITADEL is an open source identity management platform. From 2.71.11 to before 3.4.10 and 4.15.0, a vulnerability was discovered in Zitadel's LDAP identity provider implementation, which fails to properly escape user-provided usernames before incorporating them into LDAP search filters. This allows unauthenticated attackers to perform LDAP Filter Injection during the login process. While this vulnerability does not allow for a full authentication bypass, an attacker can use LDAP metacharacters (such as *, (,)) to perform blind LDAP injection. By observing the different failure (or success) responses, an attacker can systematically enumerate valid usernames and extract sensitive attribute data from the connected LDAP directory. This vulnerability is fixed in 3.4.10 and 4.15.0.	7.5	More Details
CVE-2021-47942	Home Assistant Community Store (HACS) 1.10.0 contains a path traversal vulnerability that allows unauthenticated attackers to read sensitive files by traversing directories via the /hacsfiles/ endpoint. Attackers can retrieve the .storage/auth file containing user credentials and refresh tokens, then craft valid JWT tokens to gain administrative access to Home Assistant instances.	7.5	More Details
CVE-2026-6514	The InfusedWoo Pro plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 5.1.2 via the popup_submit. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.5	More Details
CVE-2025-28343	striso-control-firmware 54c9722 is vulnerable to Buffer Overflow in function ThreadReadButtons.	7.5	More Details
CVE-2026-8954	Incorrect boundary conditions, integer overflow in the Audio/Video component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.5	More Details
CVE-2025-28344	striso-control-firmware 54c9722 is vulnerable to Buffer Overflow in function AuxJack.	7.5	More Details
CVE-2026-44289	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs could recurse without a depth limit while decoding nested protobuf data. This affected both skipping unknown group fields and generated decoding of nested message fields. A crafted protobuf binary payload could cause the JavaScript call stack to be exhausted during decoding. This vulnerability is fixed in 7.5.6 and 8.0.2.	7.5	More Details
CVE-2026-44432	urllib3 is an HTTP client library for Python. From 2.6.0 to before 2.7.0, urllib3 could decompress the whole response instead of the requested portion (1) during the second HTTPResponse.read(amt=N) call when the response was decompressed using the official Brotli library or (2) when HTTPResponse.drain_conn() was called after the response had been read and decompressed partially (compression algorithm did not matter here). These issues could cause urllib3 to fully decode a small amount of highly compressed data in a single operation. This could result in excessive resource consumption (high CPU usage and massive memory allocation for the decompressed data) on the client side. This vulnerability is fixed in 2.7.0.	7.5	More Details
CVE-2026-31910	Server-Side Request Forgery (SSRF) vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	7.5	More Details
CVE-2020-37220	Huawei HG630 V2 router contains an authentication bypass vulnerability that allows unauthenticated attackers to obtain administrative access by retrieving the device serial number. Attackers can query the /api/system/deviceinfo endpoint without authentication to extract the SerialNumber field, then use the last 8 characters as the default password to login to the router.	7.5	More Details
CVE-2026-6381	The WP Maps WordPress plugin before 4.9.3 does not properly sanitize a parameter before using it in a file path, allowing authenticated users to perform Local File Inclusion attacks.	7.5	More Details
CVE-2026-8964	Spoofing issue in the Popup Blocker component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	7.5	More Details
CVE-2026-8963	Spoofing issue in the Web Speech component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	7.5	More Details
CVE-2026-41552	PDF Export Module used in DHTMLX's products Gantt and Scheduler is vulnerable to Path Traversal due to lack of HTML sanitization. An unauthenticated user could craft the html payload which could include local files from the server and display them in the generated PDF. This issue was fixed in PDF Export Module version 0.7.6.	7.5	More Details
CVE-2026-39079	An issue in prestashop upsshipping all versions through at least 2.4.0 allows a remote attacker to obtain sensitive information via the /modules/upsshipping/logs/, and /modules/upsshipping/lib/UPSBaseApi.php components	7.5	More Details
CVE-2026-8960	Spoofing issue in WebExtensions. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	7.5	More Details
CVE-2026-6403	The Quick Playground plugin for WordPress is vulnerable to Path Traversal in versions up to and including 1.3.3. This is due to insufficient path validation in the qckply_zip_theme() function, which appends a user-controlled 'stylesheet' parameter directly to the theme root directory path without sanitizing directory traversal sequences. This makes it possible for unauthenticated attackers to trigger the creation of a ZIP archive containing arbitrary files from the server's filesystem — including wp-config.	7.5	More Details
CVE-2026-42009	A flaw was found in gnutls. A remote attacker could exploit an issue in the Datagram Transport Layer Security (DTLS) packet reordering logic. The comparator function, responsible for ordering DTLS packets by sequence numbers, did not correctly handle packets with duplicate sequence numbers. This could lead to unstable packet ordering or undefined behavior, resulting in a denial of service.	7.5	More Details
CVE-2026-44478	hoppscotch is an open source API development ecosystem. The fix for CVE-2026-28215 in version 2026.2.0 addresses the unauthenticated POST /v1/onboarding/config endpoint by checking onboardingCompleted and canReRunOnboarding before allowing config overwrites. However, GET /v1/onboarding/config still leaks all infrastructure secrets in plaintext to unauthenticated users when the ONBOARDING_RECOVERY_TOKEN stored in the database is an empty string. This vulnerability is fixed in 2026.4.0.	7.5	More Details

CVE-2026-46419	Yubico webauthn-server-core (aka java-webauthn-server) 2.8.0 before 2.8.2 incorrectly checks a function's return value in the second factor flow, leading to impersonation.	7.5	More Details
CVE-2025-15609	The Fortis for WooCommerce WordPress plugin before 1.3.1 may leak sensitive API keys to unauthenticated attackers, allowing them to query Fortis' API and retrieve sensitive customer information, like past orders, PII, etc.	7.5	More Details
CVE-2026-8813	This affects versions of the package exifreader before 4.39.0. A crafted image containing an ICC mluc tag can set an attacker-controlled record count together with a zero record size. During parsing, ExifReader repeatedly processes the same record and appends entries to an array without sufficient bounds validation, causing excessive memory growth. In applications that parse attacker-supplied images, this may lead to denial of service through memory exhaustion.	7.5	More Details
CVE-2025-14869	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.5 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to cause denial of service by sending specially crafted payloads on certain API endpoints.	7.5	More Details
CVE-2025-14870	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.5 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to cause denial of service by sending specially crafted JSON payloads due to insufficient input validation.	7.5	More Details
CVE-2020-37219	Joomla com_fabrik 3.9.11 contains a directory traversal vulnerability that allows unauthenticated attackers to list arbitrary files by manipulating the folder parameter. Attackers can send GET requests to the onAjax_files method with path traversal sequences to enumerate files in system directories outside the intended web root.	7.5	More Details
CVE-2026-27886	Strapi is an open source headless content management system. Strapi versions starting in 4.0.0 and prior to 5.37.0 did not sufficiently sanitize query parameters when filtering content via relational fields. An unauthenticated attacker could use the `where` query parameter on any publicly-accessible content-type with an `updatedBy` (or other admin-relation) field to perform a boolean-oracle attack against private fields on the joined `admin_users` table, including the `resetPasswordToken` field. Extracting an admin reset token via this oracle made full administrative account takeover possible without authentication. When a filter such as `where[updatedBy][resetPasswordToken][$startsWith]=a` was applied to a public Content API endpoint, the underlying query generation performed a `LEFT JOIN` against the `admin_users` table and emitted a `WHERE` clause referencing the joined column. The query parameter sanitization layer did not block operator chains that traversed into relational target schemas the caller had no read permission on, allowing the response count to be used as a one-bit oracle on any admin-table field. The patch in version 5.37.0 introduces explicit query-parameter sanitization at the controller and service boundary via three new primitives: `strictParam`, `addQueryParams`, and `addBodyParams`. Operator chains that traverse into restricted relational targets are now rejected before reaching the database.	7.5	More Details
CVE-2026-31909	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	7.5	More Details
CVE-2021-47969	Color Notes 1.4 contains a denial of service vulnerability that allows attackers to crash the application by pasting excessively long character strings into note fields. Attackers can generate a payload containing 350,000 repeated characters and paste it twice into a new note to cause the application to stop responding.	7.5	More Details
CVE-2026-4029	The Database Backup for WordPress plugin for WordPress is vulnerable to unauthorized database export in all versions up to, and including, 2.5.2. This is due to the plugin not properly enforcing the return value of its authorization check. This makes it possible for unauthenticated attackers to export database tables, leading to Sensitive Information Exposure. Note: This vulnerability is only exploitable in WordPress Multisite environments where the deprecated is_site_admin() function exists.	7.5	More Details
CVE-2021-47971	My Notes Safe 5.3 contains a denial of service vulnerability that allows attackers to crash the application by pasting excessively long character strings into note fields. Attackers can generate a payload containing 350000 repeated characters and paste it twice into a new note to trigger an application crash.	7.5	More Details
CVE-2026-4031	The Database Backup for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.5.2. This is due to the plugin not restricting access to the wp_db_temp_dir parameter, which controls where database backups are written. This makes it possible for unauthenticated attackers to send a request to wp-cron.php with a poisoned wp_db_temp_dir value pointing to a publicly accessible directory (e.g., wp-content/uploads/), and if a scheduled backup is due, intercept the backup file before it is cleaned up. The backup file has a predictable name based on the database name, table prefix, date, and Swatch Internet Time, making interception reliable. Successful exploitation leads to Sensitive Information Exposure including database credentials, user password hashes, and personally identifiable information. This vulnerability requires that the site administrator has configured scheduled backups.	7.5	More Details
CVE-2026-40423	When a SIP profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-8521	Use after free in Tab Groups in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	7.5	More Details
CVE-2026-40629	When SSL profiles are configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-41218	When BIG-IP PEM iRules are configured on a virtual server (iRules using commands starting with CLASSIFICATION::, CLASSIFY::, PEM::, PSC::, and the urlcatquery command), undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-41227	On an HTTP/2 virtual server with Layer 7 DoS Protection configured, undisclosed traffic can result in an increase in memory consumption causing the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-8510	Integer overflow in Skia in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	7.5	More Details

CVE-2018-25329	WordPress Plugin WP with Spritz 1.0 contains a remote file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by injecting file paths into the url parameter. Attackers can send GET requests to wp.spritz.content.filter.php with malicious url values to access sensitive files like system configuration and credentials.	7.5	More Details
CVE-2026-41956	When a classification profile is configured on a UDP virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-46356	Fleet is open source device management software. Prior to version 4.80.1, a vulnerability in Fleet's IP extraction logic allows unauthenticated attackers to bypass API rate limiting by spoofing client IP headers. This may allow brute-force login attempts or other abuse against Fleet instances exposed to the public internet. Fleet extracted client IP addresses from request headers (`True-Client-IP`, `X-Real-IP`, `X-Forwarded-For`) without validating that those headers originate from a trusted proxy. The extracted IP is used as the key for rate limiting and IP ban decisions. As a result, an attacker could rotate the value of these headers on each request, causing Fleet to treat each attempt as coming from a different client. This effectively bypasses per-IP rate limits on sensitive endpoints such as the login API, enabling unrestricted brute-force or credential stuffing attacks. This issue primarily affects Fleet instances that are directly exposed to the internet without a reverse proxy that overwrites forwarded-IP headers. Instances behind a properly configured proxy or WAF are less affected. Version 4.80.1 contains a patch. If an immediate upgrade is not possible, administrators should ensure Fleet is deployed behind a reverse proxy (e.g., nginx, Cloudflare, AWS ALB) that overwrites `X-Forwarded-For` with the true client IP, and apply rate limiting at the proxy or WAF layer.	7.5	More Details
CVE-2018-25326	Google Drive for WordPress 2.2 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by injecting directory traversal sequences in the file_name parameter. Attackers can send POST requests to gdrive-ajaxs.php with the ajaxstype parameter set to del_fl_bkp and file_name containing traversal sequences ../../wp-config.php to access sensitive configuration files.	7.5	More Details
CVE-2026-42409	When an HTTP/2 profile and an iRule containing the HTTP::redirect or HTTP::respond command are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-42334	Mongoose is a MongoDB object modeling tool designed to work in an asynchronous environment. Prior to 6.13.9, 7.8.9, 8.22.1, and 9.1.6, a vulnerability allows bypassing Mongoose’s sanitizeFilter query sanitization mechanism via the $nor operator. When sanitizeFilter is enabled, Mongoose wraps query operators in $eq to neutralize them. However, prior to the fix, $nor was not included in the set of logical operators that are recursively sanitized. Because $nor accepts an array (like $and and $or), and arrays do not trigger hasDollarKeys(), malicious operators such as $ne, $gt, or $regex could be injected inside a $nor clause without being sanitized. This vulnerability is fixed in 6.13.9, 7.8.9, 8.22.1, and 9.1.6.	7.5	More Details
CVE-2026-42920	When a Client SSL profile is configured with Allow Dynamic Record Sizing on a UDP virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2018-25325	Woocommerce CSV Importer 3.3.6 contains a path traversal vulnerability that allows any registered user to delete arbitrary files by submitting unescaped filenames through the delete_export_file AJAX action. Attackers can craft POST requests with directory traversal sequences in the filename parameter to delete sensitive files like wp-config.php outside the intended export directory.	7.5	More Details
CVE-2026-7307	A flaw was found in Keycloak. A remote, unauthenticated attacker can send a specially crafted XML input to the Security Assertion Markup Language (SAML) endpoint. This malicious input can cause high CPU usage and worker thread starvation, leading to a Denial of Service (DoS) where the server becomes unavailable.	7.5	More Details
CVE-2026-7507	A session fixation vulnerability was found in Keycloak's login-actions endpoints. An unauthenticated attacker could exploit this flaw by pre-creating an authentication session and tricking a victim into visiting a maliciously crafted link. By leveraging the /login-actions/restart endpoint—which processes session handles without adequate CSRF protection or cookie ownership validation—an attacker can reset the authentication flow state. This causes Single Sign-On (SSO) to authenticate the victim transparently upon clicking the link, allowing the attacker to hijack the required-action form without needing the victim's credentials. A successful exploit could lead to complete account takeover, including highly privileged administrative accounts.	7.5	More Details
CVE-2026-6276	Using libcurl, when a custom `Host:` header is first set for an HTTP request and a second request is subsequently done using the same *easy handle* but without the custom `Host:` header set, the second request would use stale information and pass on cookies meant for the first host in the second request. Leak them.	7.5	More Details
CVE-2026-23998	Fleet is open source device management software. Prior to version 4.81.0, a vulnerability in Fleet’s Windows MDM management endpoint could allow requests to be processed without proper client certificate validation. In certain circumstances, this could allow an attacker to impersonate an enrolled Windows device and retrieve sensitive configuration data. Fleet’s Windows MDM management endpoint relies on mutual TLS (mTLS) client certificates to authenticate enrolled devices. In affected versions, requests that did not present a client certificate could be incorrectly treated as trusted. As a result, an attacker with prior knowledge of a valid enrolled device identifier could potentially impersonate that device and receive configuration payloads intended for it. These payloads may contain sensitive information such as Wi-Fi or VPN configuration data, certificates, or other secrets delivered through MDM profiles. This issue does not allow enrollment of new devices, administrative access to Fleet, or compromise of the Fleet control plane. Impact is limited to the targeted Windows device. Version 4.81.0 contains a patch. If an immediate upgrade is not possible, affected Fleet users should temporarily disable Windows MDM.	7.5	More Details
CVE-2026-40618	When an SSL profile is configured on a virtual server on BIG-IP Virtual Edition (VE) without Intel QuickAssist Technology (QAT) or on BIG-IP hardware platforms with the database variable crypto.hwacceleration set to disabled, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-40067	When a BIG-IP APM access policy is configured on a virtual server, undisclosed traffic can cause the apmd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2021-47970	Macaron Notes 5.5 contains a denial of service vulnerability that allows attackers to crash the application by creating notes with excessively long character strings. Attackers can generate a payload containing 350000 repeated characters and paste it into a note field to trigger application crash and stop functionality.	7.5	More Details
CVE-2026-	When a BIG-IP Advanced WAF or ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details

40060			
CVE-2026-8949	Integer overflow in the Widget: Win32 component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.5	More Details
CVE-2026-8336	After invoking $_internalJsEmit, which is not intended to be directly accessible, or mapreduce command’s map function in a certain way, an authenticated user can subsequently crash mongod when the server-side JavaScript engine (through $where, $function, mapreduce reduce stage, etc.) is used also in a specific way, resulting in a post-authentication denial-of-service. This issue impacts MongoDB Server v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	7.5	More Details
CVE-2021-47972	Sticky Notes & Color Widgets 1.4.2 contains a denial of service vulnerability that allows attackers to crash the application by creating notes with excessively long character strings. Attackers can paste large payloads of repeated characters into note fields to trigger application crashes and make the application stop responding.	7.5	More Details
CVE-2021-47973	Sticky Notes Widget 3.0.6 contains a denial of service vulnerability that allows attackers to crash the application by pasting excessively long character strings into note fields. Attackers can generate a payload containing 350000 repeated characters and paste it twice into a new note to trigger an application crash on iOS devices.	7.5	More Details
CVE-2026-6479	Uncontrolled recursion in PostgreSQL SSL and GSS negotiation allows an attacker able to connect to a PostgreSQL AF_UNIX socket to achieve sustained denial of service. If SSL and GSS are both disabled, an attacker can do the same via access to a PostgreSQL TCP socket. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	7.5	More Details
CVE-2026-8073	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation and missing capability check in the 'downloadZIP' function in all versions up to, and including, 6.0.6. This makes it possible for unauthenticated attackers to read and delete arbitrary files limited in the WordPress uploads base directory.	7.5	More Details
CVE-2026-8946	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.5	More Details
CVE-2026-8945	Sandbox escape in Firefox and Firefox Focus for Android. This vulnerability was fixed in Firefox 151.	7.5	More Details
CVE-2026-8557	Use after free in Accessibility in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2021-47977	WordPress Plugin Anti-Malware Security and Bruteforce Firewall 4.20.59 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the file parameter. Attackers can send requests to the duplicator_download action via admin-ajax.php with path traversal sequences to access sensitive system files outside the intended directory.	7.5	More Details
CVE-2026-42186	OpenBao is an open source identity-based secrets management system. Prior to 2.5.3, when OpenBao's initial namespace deletion fails, subsequent retries fail to properly remove all data before marking the namespace as deleted. This can affect any outstanding leases as well as potentially leaving unrelated storage entries around. This vulnerability is fixed in 2.5.3.	7.5	More Details
CVE-2026-44216	Wasmtime is a runtime for WebAssembly. From 30.0.0 to 36.0.8, 43.0.2, and 44.0.1, Wasmtime's allocation logic for a WebAssembly table contained checked arithmetic which panicked on overflow. This overflow is possible to trigger, and thus panic, when a table with an extremely large size is allocated. This is possible with the WebAssembly memory64 proposal where tables can have sizes in the 64-bit range as opposed to the previous 32-bit range which would not overflow. The panic happens when attempting to create a very large table, such as when instantiating a WebAssembly module or component. This vulnerability is fixed in 36.0.8, 43.0.2, and 44.0.1.	7.5	More Details
CVE-2026-44375	Nerdbank.MessagePack is a NativeAOT-compatible MessagePack serialization library. Prior to 1.1.62, Nerdbank.MessagePack contains an uncontrolled stack allocation vulnerability in DateTime decoding. A malicious MessagePack payload can declare an oversized timestamp extension length, causing the reader to allocate an attacker-controlled number of bytes on the stack. This can trigger a StackOverflowException, which is not catchable by user code and terminates the process. This vulnerability is fixed in 1.1.62.	7.5	More Details
CVE-2026-8547	Insufficient policy enforcement in Passwords in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-42594	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, the webhook middleware spawns a goroutine that holds a reference to the request's echo.Context after the synchronous handler returns ErrAsyncProcess and Echo recycles the context back to its sync.Pool. When a concurrent request claims the recycled context, c.Reset() clears the store. If the webhook goroutine reaches hardTimeoutMiddleware at that moment, an unchecked type assertion on a nil store entry panics outside any recover() scope, crashing the Gotenberg process. Any anonymous caller reaches the webhook path (default webhook-deny-list filters only the webhook destination, not the submitter). A single-source stress of ~24 webhook requests plus ~60 GET /version requests crashes the process in about two seconds. This vulnerability is fixed in 8.32.0.	7.5	More Details
CVE-2026-39455	When the BIG-IP Configuration utility is configured to use Lightweight Directory Access Protocol (LDAP) authentication, undisclosed traffic can cause the httpd process to exhaust the available file descriptors. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-39458	When a BIG-IP DNS profile enabled with DNS cache is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-38728	An issue in Nodemailer smtp_server before v.3.18.3 allows a remote attacker to cause a denial of service via the SMTPStream._write, lib/smtp-stream.js components	7.5	More Details
CVE-	The Contest Gallery plugin for WordPress is vulnerable to SQL Injection via the 'form_input' parameter in versions up to, and including, 28.1.6. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query inside the unauthenticated 'post_cg_gallery_form_upload' AJAX action (specifically the 'cb' branch of the included users-upload-		More

2026-8912	check.php, where $f_input_id is concatenated unquoted into 'SELECT Field_Content FROM ... WHERE id = $f_input_id'). The endpoint is gated only by a public frontend nonce ('cg1l_action' / 'cg_nonce') that is exposed in the page source of any public gallery page. 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	Details
CVE-2026-42304	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to 26.4.0rc2, the twisted.names module is vulnerable to a Denial of Service (DoS) attack via resource exhaustion during DNS name decompression. A remote, unauthenticated attacker can exploit this by sending a crafted TCP DNS packet containing deeply chained compression pointers. This flaw bypasses previous loop-prevention logic, causing the single-threaded Twisted reactor to hang while processing millions of recursive lookups, effectively freezing the server. This vulnerability is fixed in 26.4.0rc2.	7.5	More Details
CVE-2026-47100	Funnel Builder for WooCommerce Checkout prior to 3.15.0.3 contains a missing authorization vulnerability in the public checkout endpoint that allows unauthenticated attackers to invoke internal methods and write arbitrary data to the plugin's External Scripts global setting. Attackers can inject malicious JavaScript through the External Scripts setting that executes in the browsers of all checkout page visitors.	7.5	More Details
CVE-2026-43634	HestiaCP versions 1.2.0 through 1.9.4 contain an IP spoofing vulnerability that allows unauthenticated remote attackers to bypass authentication security controls by supplying an arbitrary IP address in the CF-Connecting-IP HTTP header without verifying the request originated from Cloudflare's network. Attackers can exploit this to circumvent fail2ban brute-force protection, bypass per-user IP allowlists, and poison authentication audit logs by spoofing trusted IP addresses on each request.	7.5	More Details
CVE-2026-46359	phpMyFAQ before 4.1.2 contains a sql injection vulnerability in CurrentUser::setTokenData that allows authenticated attackers to execute arbitrary SQL by injecting malicious OAuth token claims. Attackers with Azure AD accounts containing SQL metacharacters in display names or JWT claims can break out of string literals and execute arbitrary database queries.	7.5	More Details
CVE-2026-29963	HSC MailInspector 5.3.3-7 has a Path Traversal vulnerability due to improper validation of user-supplied input in the /tap/dw.php endpoint. The text parameter is used to construct file paths without adequate normalization or restriction to a safe base directory. A remote attacker can exploit this flaw to access arbitrary files on the underlying operating system, resulting in unauthorized disclosure of sensitive information.	7.5	More Details
CVE-2026-4798	The Avada Builder plugin for WordPress is vulnerable to time-based SQL Injection via the ‘product_order’ parameter in all versions up to, and including, 3.15.1 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. Note: The vulnerability can only be exploited if WooCommerce was previously used and then deactivated.	7.5	More Details
CVE-2026-33232	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Versions 0.4.2 through 0.6.51 are vulnerable to an unauthenticated Denial of Service (DoS) through the server due to uncontrolled disk space consumption. The download_agent_file endpoint creates persistent temporary files for every request but fails to delete them after they are served. An unauthenticated attacker can repeatedly call this endpoint to exhaust the server's disk space, causing the database or other system services to fail due to "No space left on device" errors, rendering the entire AutoGPT Platform backend unavailable to all users. This issue has been patched in version 0.6.52.	7.5	More Details
CVE-2026-44575	Next.js is a React framework for building full-stack web applications. From 15.2.0 to before 15.5.16 and 16.2.5, App Router applications that rely on middleware or proxy-based checks for authorization can allow unauthorized access through transport-specific route variants used for segment prefetching. In affected configurations, specially crafted .rsc and segment-prefetch URLs can resolve to the same page without being matched by the intended middleware rule, which can allow protected content to be reached without the expected authorization check. This vulnerability is fixed in 15.5.16 and 16.2.5.	7.5	More Details
CVE-2026-44714	The bitcoinj library is a Java implementation of the Bitcoin protocol. Prior to 0.17.1, ScriptExecution.correctlySpends() contains two fast-path verification bugs for standard P2PKH and native P2WPKH spends in core/src/main/java/org/bitcoinj/script/ScriptExecution.java. In both branches, bitcoinj verifies an attacker-controlled signature/public-key pair but fails to verify that the public key is the one committed to by the output being spent. As a result, any attacker keypair can satisfy bitcoinj's local verification for arbitrary P2PKH and P2WPKH outputs. This vulnerability is fixed in 0.17.1.	7.5	More Details
CVE-2026-44573	Next.js is a React framework for building full-stack web applications. From 12.2.0 to before 15.5.16 and 16.2.5, Applications using the Pages Router with i18n configured and middleware/proxy-based authorization can allow unauthorized access to protected page data through locale-less /_next/data/<buildId>/<page>.json requests. In affected configurations, middleware does not run for the unprefixed data route, allowing an attacker to retrieve SSR JSON for protected pages without passing the intended authorization checks. This vulnerability is fixed in 15.5.16 and 16.2.5.	7.5	More Details
CVE-2026-29962	HSC MailInspector v5.3.3-7 contains a Local File Inclusion (LFI) vulnerability caused by improper control of user-supplied file paths. The endpoint /vendor/phpunit/phpunit.php processes user-controlled parameters that directly affect file access operations without adequate validation, sanitization, or path restriction. This allows a remote attacker to exploit Path Traversal techniques to read arbitrary files from the underlying operating system and application directories, leading to sensitive information disclosure.	7.5	More Details
CVE-2025-27850	The locally served web site on the Garmin WDU (v1 1.4.6 and v2 5.0) allows a symlink attack. If a malicious graphics package containing symlinks is uploaded, the web server follows the supplied links when serving content. No mechanisms to restrict those link targets to a specific area of the filesystem is enabled. This allows an attacker to retrieve arbitrary files from the device.	7.5	More Details
CVE-2026-8696	radare2 6.1.5 contains a use-after-free vulnerability in the gdbr_pids_list() function within the GDB client core that allows remote attackers to cause a denial of service or potentially execute arbitrary code by sending malformed thread information responses. Attackers can trigger the vulnerability by causing qsThreadInfo to fail after qfThreadInfo successfully allocates RDebugPid structures, resulting in double-free memory corruption when the error path attempts to clean up the list.	7.5	More Details
CVE-2026-42587	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, HttpContentDecompressor accepts a maxAllocation parameter to limit decompression buffer size and prevent decompression bomb attacks. This limit is correctly enforced for gzip and deflate encodings via ZlibDecoder, but is silently ignored when the content encoding is br (Brotli), zstd, or snappy. An attacker can bypass the configured decompression limit by sending a compressed payload with Content-Encoding: br instead of Content-Encoding: gzip, causing unbounded memory allocation and out-of-memory denial of service. The same vulnerability exists in DelegatingDecompressorFrameListener for HTTP/2 connections. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	7.5	More Details
CVE-2026-42577	Netty is an asynchronous, event-driven network application framework. From 4.2.0.Final to 4.2.13.Final , Netty's epoll transport fails to detect and close TCP connections that receive a RST after being half-closed, leading to stale channels that are never cleaned up and, in some code paths, a 100% CPU busy-loop in the event loop thread. This vulnerability is fixed in 4.2.13.Final.	7.5	More Details

CVE-2026-42578	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, Netty's HttpProxyHandler constructs HTTP CONNECT requests with header validation explicitly disabled. The newInitialMessage() method creates headers using DefaultHttpHeadersFactory.headersFactory().withValidation(false), then adds user-provided outboundHeaders without any CRLF validation. This allows an attacker who can influence the outbound headers to inject arbitrary HTTP headers into the CONNECT request sent to the proxy server. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	7.5	More Details
CVE-2026-42579	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, Netty's DNS codec does not enforce RFC 1035 domain name constraints during either encoding or decoding. This creates a bidirectional attack surface: malicious DNS responses can exploit the decoder, and user-influenced hostnames can exploit the encoder. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	7.5	More Details
CVE-2026-44826	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.2, Vvveb CMS does not validate the sign of the quantity parameter on the cart-add endpoint. Submitting a negative integer is accepted by the server and treated as a normal positive line-item, but with the sign carried through into every downstream computation: line total, sub-total, taxes, and grand total all become negative numbers. The customer-facing cart UI then displays a negative grand total to the user, the checkout flow accepts the negative cart, and the resulting order is persisted in the merchant's database with a negative total column. From the merchant's order management dashboard, this surfaces as a real order with a negative total — an "the merchant owes the customer money" record that no legitimate workflow ever creates. This vulnerability is fixed in 1.0.8.2.	7.5	More Details
CVE-2026-42551	Flight is an extensible micro-framework for PHP. Prior to 3.18.1, Request::getMethod() unconditionally honors the X-HTTP-Method-Override header and the $_REQUEST['_method'] parameter on any HTTP verb (including safe verbs such as GET), with no opt-in and no whitelist of permitted target methods. A GET request can silently become a DELETE or PUT, enabling CSRF escalation against destructive endpoints, bypass of middleware gated on unsafe verbs, and cache poisoning between CDN and origin. This vulnerability is fixed in 3.18.1.	7.5	More Details
CVE-2026-42552	Flight is an extensible micro-framework for PHP. Prior to 3.18.1, the default error handler Engine::_error() writes the full exception message, exception code, and stack trace (including absolute filesystem paths) directly into the HTTP 500 response, with no debug gating. Production deployments leak internal paths, any secret interpolated into an exception message, and full module structure — giving attackers primitives for chaining other weaknesses (LFI, path traversal). This vulnerability is fixed in 3.18.1.	7.5	More Details
CVE-2026-42582	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final, when decoding header blocks, the non-Huffman branch of io.netty.handler.codec.http3.QpackDecoder#decodeHuffmanEncodedLiteral may execute new byte[length] for a string literal before verifying that length bytes are actually present in the compressed field section. The wire encoding allows a very large length to be expressed in few bytes. There is no check that length <= in.readableBytes() before new byte[length]. This vulnerability is fixed in 4.2.13.Final.	7.5	More Details
CVE-2021-47959	WordPress Plugin WPGraphQL 1.3.5 contains a denial of service vulnerability that allows unauthenticated attackers to exhaust server resources by sending batched GraphQL queries with duplicated fields. Attackers can send POST requests to the GraphQL endpoint with amplified field duplication payloads to trigger server out-of-memory conditions and MySQL connection errors.	7.5	More Details
CVE-2026-42583	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, Lz4FrameDecoder allocates a ByteBuf of size decompressedLength (up to 32 MB per block) before LZ4 runs. A peer only needs a 21-byte header plus compressedLength payload bytes - 22 bytes if compressedLength == 1 - to force that allocation. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	7.5	More Details
CVE-2026-42561	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.27, python-multipart has a denial of service vulnerability in multipart part header parsing. When parsing multipart/form-data, MultipartParser previously had no limit on the number of part headers or the size of an individual part header. An attacker could send a request with either many repeated headers without terminating the header block or a single very large header value, causing excessive CPU work before request rejection or completion. This vulnerability is fixed in 0.0.27.	7.5	More Details
CVE-2025-61081	In BYD Atto3, an attacker can obtain an authentication key through Brute Force attack, which is permanently available. The authentication key enables flash to the Electronic Parking Break (EPB) and Supplemental Restoration System (SRS) related ECUs.	7.5	More Details
CVE-2026-45109	Next.js is a React framework for building full-stack web applications. From 15.2.0 to before 15.5.18 and 16.2.6, it was found that the fix addressing CVE-2026-44575 did not apply to middleware.ts with Turbopack. This vulnerability is fixed in 15.5.18 and 16.2.6.	7.5	More Details
CVE-2026-47358	Terrascan v1.18.3 and prior are vulnerable to Server-Side Request Forgery (SSRF) via external URL resolution in uploaded IaC templates when running in server mode. When Terrascan parses uploaded ARM templates or CloudFormation templates, it resolves external URLs referenced within those templates via hashicorp/go-getter with all default detectors enabled, including FileDetector. An unauthenticated remote attacker can upload an ARM template containing a templateLink.uri or parametersLink.uri field, or a CloudFormation template containing an AWS::CloudFormation::Stack TemplateURL field, pointing to an attacker-controlled URL. Terrascan will fetch the attacker-controlled URL server-side. Unlike SSRF via the remote scan endpoint, file:// URLs are directly usable without requiring an X-Terraform-Get redirect, enabling local file read. This affects deployments running terrascan in server mode (terrascan server), which binds to 0.0.0.0 with no authentication. Note: Terrascan was archived in August 2023 and no patch will be released.	7.5	More Details
CVE-2026-46366	phpMyFAQ before 4.1.2 contains an information disclosure vulnerability in the getIdFromSolutionId() method that lacks permission filtering, allowing unauthenticated attackers to enumerate restricted FAQ entries and read their titles via the /solution_id_{id}.html endpoint. Attackers can sequentially iterate solution IDs to discover all FAQs including those restricted to specific users or groups, leaking sensitive metadata through redirect Location headers and page canonical links.	7.5	More Details
CVE-2026-47357	Terrascan v1.18.3 and prior are vulnerable to Server-Side Request Forgery (SSRF) via the remote_url parameter in the remote directory scan endpoint (POST /v1/{iac}/{iacVersion}/{cloud}/remote/dir/scan) when running in server mode. An unauthenticated remote attacker can supply an attacker-controlled HTTP URL as remote_url with remote_type set to "http". The URL is passed directly to hashicorp/go-getter (v1.7.5) without validation. Go-getter's HttpGetter supports the X-Terraform-Get response header, allowing the attacker's server to redirect the download to a file:// URL, enabling local file read. Additionally, HttpGetter has Netrc set to true, causing it to read ~/.netrc and send stored credentials to attacker-controlled hostnames. This affects deployments running terrascan in server mode (terrascan server), which binds to 0.0.0.0 with no authentication. Note: Terrascan was archived in August 2023 and no patch will be released.	7.5	More Details
CVE-	Terrascan v1.18.3 and prior are vulnerable to Server-Side Request Forgery (SSRF) via the webhook_url parameter in the file scan endpoint (POST /v1/{iac}/{iacVersion}/{cloud}/local/file/scan) when running in server mode. An unauthenticated remote attacker can supply an arbitrary URL as the webhook_url multipart form parameter. After scanning the uploaded file, Terrascan sends an HTTP POST		More

2026-47356	request to the attacker-controlled URL containing the full scan results as a JSON body, with the attacker-supplied webhook_token forwarded as a Bearer token in the Authorization header. The retryable HTTP client retries up to 10 times on failure. This affects deployments running terrascan in server mode (terrascan server), which binds to 0.0.0.0 with no authentication. Note: Terrascan was archived in August 2023 and no patch will be released.	7.5	Details
CVE-2026-46474	Trog::TOTP versions before 1.006 for Perl generate secrets using rand. Secrets were generated using Perl's built-in rand function, which is predictable and unsuitable for security usage.	7.5	More Details
CVE-2026-45398	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, _validate_collection_access() checks the user-memory-* and file-* collection name prefixes but does not check knowledge base collections, which use raw UUIDs as collection names. Any authenticated user who knows a private knowledge base UUID can read its content through the retrieval query endpoints, even though the knowledge API correctly denies that user access. The same gap affects the retrieval write endpoints (/process/text, /process/file, /process/files/batch, /process/web, /process/youtube), allowing an attacker to inject content into or overwrite another user's knowledge base. This vulnerability is fixed in 0.9.5.	7.5	More Details
CVE-2026-44579	Next.js is a React framework for building full-stack web applications. From to before 15.5.16 and 16.2.5, applications using Partial Prerendering through the Cache Components feature can be vulnerable to connection exhaustion through crafted POST requests to a server action. In affected configurations, a malicious request can trigger a request-body handling deadlock that leaves connections open for an extended period, consuming file descriptors and server capacity until legitimate users are denied service. This vulnerability is fixed in 15.5.16 and 16.2.5.	7.5	More Details
CVE-2026-8968	Denial-of-service due to invalid pointer in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.5	More Details
CVE-2025-56352	In tinyMQTT commit 6226ade15bd4f97be2d196352e64dd10937c1962 (2024-02-18), the broker mishandles protocol violations during CONNECT packet parsing. When receiving a CONNECT packet with a zero-length Client ID while CleanSession is set to 0, the broker correctly replies with a CONNACK return code 0x02 (Identifier Rejected) but fails to explicitly close the TCP connection. Since the surrounding connection teardown logic is not guaranteed to execute, each such invalid CONNECT attempt leaves the underlying socket open. Repeated attempts cause server-side resource exhaustion due to accumulating file descriptors and memory usage, potentially resulting in denial of service.	7.5	More Details
CVE-2026-44004	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, sandboxed code can call Buffer.alloc() with an arbitrary size to allocate memory directly on the host heap. Because Buffer.alloc is a synchronous C++ native call, vm2's timeout option cannot interrupt it. A single request can exhaust host memory and crash the process with a FATAL ERROR: Reached heap limit. This vulnerability is fixed in 3.11.0.	7.5	More Details
CVE-2026-8686	Missing bounds validation in the MQTT v5.0 property parser in coreMQTT before 5.0.1 allows an MQTT broker to cause a denial of service by sending a crafted packet. To remediate this issue, users should upgrade to v5.0.1.	7.5	More Details
CVE-2026-8695	radare2 6.1.5 contains a use-after-free vulnerability in the gdbr_threads_list() function that allows remote attackers to trigger memory corruption by sending a valid qfThreadInfo response followed by a malformed qsThreadInfo response. Attackers can exploit this vulnerability through GDB remote debugging to cause a denial of service or potentially achieve code execution by manipulating thread list processing.	7.5	More Details
CVE-2026-5773	libcurl might in some circumstances reuse the wrong connection for SMB(S) transfers. libcurl features a pool of recent connections so that subsequent requests can reuse an existing connection to avoid overhead. When reusing a connection a range of criteria must be met. Due to a logical error in the code, a network transfer operation that was requested by an application could wrongfully reuse an existing SMB connection to the same server that was using a different 'share' than the new subsequent transfer should. This could in unlucky situations lead to the download of the wrong file or the upload of a file to the wrong place. When this happens, the same credentials are used and the server name is the same.	7.5	More Details
CVE-2026-41947	Dify version 1.14.1 and prior contains an authorization bypass vulnerability that allows authenticated editor users to set and enable trace configurations for any application regardless of tenant ownership. Attackers can exploit missing tenant ownership checks in the trace configuration endpoints to redirect all messages and responses from victim applications to attacker-controlled LLM trace providers. NOTE: Dify Cloud allows unauthenticated free self-registration, making account creation trivially accessible to any attacker.	7.4	More Details
CVE-2026-44636	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. From to 1.8.7-r1, signed integer overflow in sixel_encode_highcolor's allocation size calculation can lead to a heap buffer overflow. The public sixel_encode entry point validates only that width and height are greater than zero, with no upper bound. width and height are multiplied as plain int when computing the allocation size for paletted_pixels and normalized_pixels. Any caller that asks libsixel to encode a pixel buffer with width times height greater than INT_MAX (about 2.15 billion) will hit a wrapped allocation size; under the right wrap, the malloc succeeds with a buffer much smaller than the encoder expects, and the encoder writes past the end of the heap allocation. This vulnerability is fixed in 1.8.7-r2.	7.4	More Details
CVE-2026-44511	Katalyst Koi is a framework for building Rails admin functionality. Prior to 4.20.0 and 5.6.0, admin session cookies were not invalidated when an admin user logged out. An attacker with access to a valid admin session cookie could continue to access admin functionality after logout, until the cookie expired or session secrets were rotated. This vulnerability is fixed in 4.20.0 and 5.6.0.	7.4	More Details
CVE-2026-45245	Summarize prior to 0.15.1 contains a vulnerability in the hover summary feature that allows malicious pages to dispatch synthetic mouseover events over attacker-controlled links, causing the extension to make authenticated daemon requests using stored tokens without verifying event trustworthiness. Attackers can place local or private-network URLs behind hoverable links to route authenticated requests through the daemon, potentially accessing sensitive internal endpoints when users interact with attacker-controlled content.	7.4	More Details
CVE-2026-41132	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.10 and 2.11.5, the configured SMTP server may be spoofed with any certificate (e.g. self-signed), leaving credentials and all emails sent open to MITM attacks. This vulnerability is fixed in 2.10.10 and 2.11.5.	7.4	More Details
CVE-2026-33376	When using an IPv6 allow-list for the Auth Proxy feature, it defaults to /32 addresses. Addresses specifying a mask explicitly are not affected; to mitigate easily, add the desired mask (usually /128) to the addresses. Only auth proxy is affected; Okta, SAML, LDAP, etc are unaffected here.	7.4	More Details
CVE-2026-	Microsoft APM is an open-source, community-driven dependency manager for AI agents. From 0.5.4 to 0.12.4, two primitive integrators in apm-cli enumerate package files with bare Path.glob() / Path.rglob() calls and read each match with Path.read_text(), transparently following symbolic links. A symlink committed inside a remote APM dependency under .apm/prompts/<x>.prompt.md or .apm/agents/<x>.agent.md is preserved verbatim into apm_modules/ on clone and then dereferenced during integration, with the	7.4	More

45539	resolved content written as a regular file into the project's deploy directories. The package content_hash, the pre-deploy SecurityGate scan, and apm audit do not flag this. The deploy roots are not added to the auto-generated .gitignore, so the resulting files are staged by git add by default. This vulnerability is fixed in 0.13.0.		Details
CVE-2025-70950	An issue in gohttp commit 34ea51 allows attackers to execute a directory traversal via supplying a crafted request.	7.3	More Details
CVE-2026-44567	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.1.124, the API does not properly validate that the user has an authorized user role of user. By default, when Open WebUI is configured with new sign-ups enabled, the default user role is set to pending. In this configuration, an administrator is required to go into the Admin management panel following a new user registration and reconfigure the user to have a role of either user or admin before that user is able to access the web application. This vulnerability is fixed in 0.1.124.	7.3	More Details
CVE-2025-51427	An issue was discovered in ModelScope 1.25.0 allowing attackers to execute arbitrary code via crafted module listed in the configuration file (dey_mini.yaml) under the key ['nnet']['module'].	7.3	More Details
CVE-2026-44566	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.1.124, when attaching files to a promp, the name of the file is derived from the original HTTP upload request and is not validated or sanitized. This allows for users to upload files with names containing dot-segments in the file path and traverse out of the intended uploads directory. Effectively, users can upload files anywhere on the filesystem the user running the web server has permission. This vulnerability is fixed in 0.1.124.	7.3	More Details
CVE-2024-55045	Firmament-Autopilot FMT-Firmware commit de5aec was discovered to contain a buffer overflow via the task_mavobc_entry function at /comm/task_comm.c.	7.3	More Details
CVE-2026-22069	A local privilege escalation vulnerability exists in O+ Connect because it fails to validate the identity of the caller on the pipe interface.	7.3	More Details
CVE-2026-39054	Oinone Pamirs 7.0.0 contains a command injection vulnerability in CommandHelper.executeCommands. The method starts a shell process and writes attacker-controlled command strings directly to the process standard input without sanitization. In affected deployments, this can result in arbitrary operating system command execution.	7.3	More Details
CVE-2026-8947	Use-after-free in the DOM: Bindings (WebIDL) component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.3	More Details
CVE-2026-44549	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, Excel file attachments are previewed in an unsafe way. A crafted XLSX file payload can be used to cause the sheetjs function sheet_to_html to embed an XSS payload into the generated HTML. This is subsequently added to the DOM unsanitized via @html causing the payload to trigger. This vulnerability is fixed in 0.8.0.	7.3	More Details
CVE-2026-8771	A security flaw has been discovered in linlinjava litemall up to 1.8.0. This impacts the function list of the file litemall-wx-api/src/main/java/org/linlinjava/litemall/wx/web/WxGoodsController.java of the component Front-end WeChat API. Performing a manipulation results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-8768	A vulnerability was found in vercel ai up to 3.0.97. The affected element is the function validateDownloadUrl of the file packages/provider-utils/src/download-blob.ts of the component provider-utils. The manipulation results in server-side request forgery. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-24712	Northern.tech CFEngine Enterprise and Community before 3.21.8, 3.24.3, and 3.27.0 allows Command injection.	7.3	More Details
CVE-2026-8758	A vulnerability was determined in Metasoft 美特软件 MetaCRM up to 6.4.0 Beta06. This impacts an unknown function of the file /common/jsp/upload3.jsp. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-8757	A vulnerability was found in adenhq hive up to 0.11.0. This affects the function _read_events_tail of the file core/framework/server/routes_sessions.py of the component Delete Request Handler. Performing a manipulation results in path traversal. 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-2026-8756	A vulnerability has been found in fishaudio Bert-VITS2 up to 8f7fbd8c4770965225d258db548da27dc8dd934c. The impacted element is the function generate_config of the file webui_preprocess.py of the component Gradio Interface. Such manipulation of the argument data_dir leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-8755	A flaw has been found in fishaudio Bert-VITS2 up to 8f7fbd8c4770965225d258db548da27dc8dd934c. The affected element is the function _get_all_models of the file hiyoriUI.py of the component Model Handler. This manipulation causes path traversal. The attack can be initiated remotely. The exploit has been published and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-8725	A weakness has been identified in CoreWorxLab CAAL up to 1.6.0. The affected element is an unknown function of the file src/caal/webhooks.py of the component test-hass Endpoint. This manipulation causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
	A vulnerability was determined in Oinone Pamirs up to 7.2.0. Affected by this issue is the function		

CVE-2026-8734	RSQLToSQLNodeConnector.makeVariable of the component queryListByWrapper Interface. This manipulation causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-44721	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, a stored cross-site scripting (XSS) vulnerability that allows any authenticated user with model creation permission (workspace.models) to execute arbitrary JavaScript in the browser of any other user (including admins) who views the malicious model in the chat UI. This vulnerability is fixed in 0.9.0.	7.3	More Details
CVE-2026-8751	A security flaw has been discovered in h2oai h2o-3 up to 7402. This affects the function importBinaryModel of the file h2o-core/src/main/java/hex/Model.java of the component JAR Handler. Performing a manipulation results in deserialization. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-8759	A vulnerability was identified in xiandafu beetl up to 3.20.2. Affected is an unknown function of the file beetl-classic-integration/beetl-spring-classic/src/main/java/org/beetl/ext/spring/SpELFunction.java of the component SpELFunction. The manipulation leads to improper neutralization of special elements used in an expression language statement. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-42584	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, HttpClientCodec pairs each inbound response with an outbound request by queue.poll() once per response, including for 1xx. If the client pipelines GET then HEAD and the server sends 103, then 200 with GET body, then 200 for HEAD, the queue pairs HEAD with the first 200. The HEAD rule then skips reading that message’s body, so the GET entity bytes stay on the stream and the following 200 is parsed from the wrong offset. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	7.3	More Details
CVE-2026-32323	Mullvad VPN is a VPN client app for desktop and mobile. When using macOS with versions 2026.1 and below, Mullvad VPN may allow local privilege escalation during installation or upgrade. The installer package executes binaries from /Applications/Mullvad VPN.app without verifying if the bundle is attacker-controlled or that the path is the legitimate Mullvad application. A user in the admin group can pre-place a crafted application bundle at that location and may be able to achieve code execution as root. Since the issue only affected the installer, there is no immediate need for users to update if they are already running an older version. This issue has been fixed in version 2026.2-beta1.	7.3	More Details
CVE-2026-29226	Server-Side Request Forgery (SSRF) vulnerability in Apache OFBiz via Content component operations. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	7.3	More Details
CVE-2026-46586	Improper Control of Generation of Code ('Code Injection'), Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	7.3	More Details
CVE-2026-37430	An arbitrary file upload vulnerability in the ShopOrderImportController.java component of qihang-wms commit 75c15a allows attackers to execute arbitrary code via uploading a crafted file.	7.3	More Details
CVE-2026-8788	Net::Statsd::Lite versions through 0.10.0 for Perl allowed metric injections. The values from the set_add method were not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics. Note that version 0.9.0 fixed a similar issue CVE-2026-46719 for metric names.	7.3	More Details
CVE-2026-8970	Privilege escalation in the Security component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	7.3	More Details
CVE-2026-8785	A flaw has been found in projectworlds hospital-management-system-in-php 1.0. Affected by this vulnerability is the function getAllPatientDetail of the file update_info.php of the component GET Parameter Handler. Executing a manipulation of the argument appointment_no can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-8700	Crypt::DSA versions before 1.20 for Perl generate seeds using rand. Seeds were generated using Perl's built-in rand function, which is predictable and unsuitable for security usage.	7.3	More Details
CVE-2025-27853	The locally served web site on the Garmin WDU (v1 1.4.6 and v2 5.0) allows its authentication to be bypassed. The WDU web site only performs authentication with the client within the client's browser. The WebSockets used to communicate with the WDU server do not enforce any authentication. An attacker may bypass all authentication mechanisms by directly utilizing the remote APIs available on the websocket.	7.3	More Details
CVE-2026-26462	Offline Hospital Management System 5.3.0 allows remote code execution due to an improper Electron renderer configuration. The application enables Node.js integration while disabling context isolation, allowing JavaScript executed in the renderer process to access Node.js APIs and execute arbitrary operating system commands.	7.3	More Details
CVE-2026-39358	CubeCart is an ecommerce software solution. Prior to 6.6.0, Authenticated Time-Based Blind SQL Injection vulnerabilities were identified in the sorting parameters (sort[price], sort_activity, sort_admin, and sort_customer) of the Products and Logs endpoints in CubeCart v6.x. This allows an attacker to execute arbitrary SQL commands, compromising the confidentiality and integrity of the database. This vulnerability is fixed in 6.6.0.	7.2	More Details
CVE-2021-47975	WP Learn Manager 1.1.2 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the fieldtitle parameter. Attackers can submit POST requests to the jslm_fieldordering page with XSS payloads in the fieldtitle field to execute arbitrary JavaScript when administrators view the field ordering interface.	7.2	More Details
CVE-2026-6476	SQL injection in PostgreSQL pg_createsubscriber allows an attacker with pg_create_subscription rights to execute arbitrary SQL as a superuser. The attack takes effect when pg_createsubscriber next runs. Within major versions 17 and 18, minor versions before PostgreSQL 18.4 and 17.10 are affected. Versions before PostgreSQL 17 are unaffected.	7.2	More Details
CVE-2026-	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, the tool update endpoint (POST /api/v1/tools/id/{id}/update) is missing the workspace.tools permission check that is present on the tool create endpoint. This allows a user who has been explicitly denied tool management capabilities (and who the administrator considers untrusted for code	7.2	More

45395	execution) to replace a tool's server-side Python content and trigger execution, bypassing the intended workspace.tools security boundary. This vulnerability is fixed in 0.9.5.		Details
CVE-2026-36741	U-SPEED AC1200 Gigabit Wi-Fi Router (Model: T18-21K) V1.0 is vulnerable to Command Injection. The Network Time Protocol (NTP) configuration interface does not properly sanitize user-supplied input. An authenticated user with permission to configure NTP settings can inject arbitrary system commands through crafted input fields. These commands are executed with elevated privileges, leading to potential full system compromise.	7.2	More Details
CVE-2026-41937	Vvveb before 1.0.8.3 contains an unrestricted file upload vulnerability in the plugin upload endpoint that allows super_admin users to execute arbitrary PHP code by uploading a malicious plugin ZIP file. Attackers can craft a ZIP containing a plugin.php with a valid Slug header and a public/index.php file with arbitrary PHP code, which executes as the web server user when accessed via unauthenticated HTTP requests to the plugin's public path.	7.2	More Details
CVE-2026-39459	A vulnerability exists in iControl REST and the TMOS Shell (tmsh) where a highly privileged, authenticated attacker with at least the Manager role can create configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.2	More Details
CVE-2026-8764	A security vulnerability has been detected in H3C Magic B3 up to 100R002. This affects the function UpdateWanParams of the file /goform/aspForm. Such manipulation of the argument param leads to buffer overflow. The attack may be performed from remote. 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.	7.2	More Details
CVE-2026-3718	The ManageWP Worker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'MWP-Key-Name' HTTP request header in all versions up to, and including, 4.9.31. This is due to insufficient input sanitization and output escaping of attacker-controlled header values. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator visits the plugin's connection management page with debug parameters.	7.2	More Details
CVE-2026-45708	CubeCart is an ecommerce software solution. Prior to 6.7.3, an admin with documents edit permission can save raw <?php ... ?> into the Invoice Editor. The next time any admin clicks Print on any order, the rendered template is written to files/print.<md5>.php. files/.htaccess ships an explicit <Files print.*.php> allow from all </Files> carve-out, so the file is fetched and executed by any unauthenticated visitor. This vulnerability is fixed in 6.7.3.	7.2	More Details
CVE-2026-44380	MISP is an open source threat intelligence and sharing platform. Prior to 2.5.37, an improper access control vulnerability in the authentication key reset functionality allowed an authenticated organization administrator to reset authentication keys belonging to site administrator accounts within the same organization. Because non-site administrators were not explicitly prevented from accessing or resetting site administrator auth keys, an attacker with organization administrator privileges could potentially obtain a newly generated auth key for a higher-privileged account and use it to escalate privileges. This vulnerability is fixed in 2.5.37.	7.2	More Details
CVE-2026-6888	Successful exploitation of the SQL injection vulnerability could allow a remote authenticated attacker to execute arbitrary commands via a specific interface, potentially enabling the attacker to access, modify, or delete sensitive information within the database.	7.2	More Details
CVE-2026-6177	The Custom Twitter Feeds plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 2.5.4. This is due to insufficient output escaping in the CTF_Display_Elements::get_post_text() function when rendering cached tweet text. The plugin's ctf_get_more_posts AJAX action is available to unauthenticated users and directly outputs cached tweet data through nl2br() without HTML escaping. When an attacker can get malicious content into cached tweet data (either by tweeting content that gets cached by the site's feed configuration, or through other vulnerabilities), the malicious HTML/JavaScript is executed when the unauthenticated endpoint is accessed. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the affected endpoint.	7.2	More Details
CVE-2026-22599	Strapi is an open source headless content management system. In versions on the 4.x branch prior to 4.26.1 and on the 5.x branch prior to 5.33.2, a database-query injection vulnerability existed in the Strapi Content-Type Builder write API. An authenticated administrator could inject arbitrary database statements through the `column.defaultTo` attribute when creating or modifying a content type. Setting `defaultTo` as a tuple `[value, { isRaw: true }]` caused the value to be passed directly into Knex's `db.connection.raw()` during schema migration without sanitization, allowing arbitrary statement execution at the database layer. Depending on the database engine, this enabled arbitrary file read via database utility functions, denial of service via forced server crash on schema-migration error, and on engines that permit external program execution, remote code execution against the database server. The patch in versions 4.26.1 and 5.33.2 addresses this by restricting all Content-Type Builder write APIs to development mode only. Production deployments running v5.33.2 or later return 404 for requests against `/content-type-builder/content-types` and related endpoints, removing the network-reachable attack surface entirely.	7.2	More Details
CVE-2021-47963	Anote 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to execute arbitrary code by injecting malicious payloads into markdown files stored within the application. Attackers can craft malicious markdown files with embedded JavaScript that executes system commands when opened, enabling remote code execution on the victim's computer.	7.2	More Details
CVE-2026-27891	FacturaScripts is an open source accounting and invoicing software. Versions 2026 and below contain a critical vulnerability in the Plugins::add() function. The system fails to properly validate the file paths within uploaded ZIP archives. This allows an attacker to perform a Zip Slip attack, leading to Arbitrary File Write and Remote Code Execution (RCE) by overwriting sensitive .php files outside the designated plugins directory. The vulnerability is located in Plugins.php. While the testZipFile function attempts to validate that the ZIP contains only one root folder, it does not sanitize or validate the individual file paths within that folder. An attacker can bypass this check by naming a file ValidPluginName/../../shell.php. The explode function will see ValidPluginName as the root folder, satisfying the count($folders) != 1 check. However, during extraction, the ../../ sequence triggers a path traversal, allowing the file to be written anywhere the web server has permissions the root directory. This issue is fixed in version 2026.1.	7.2	More Details
CVE-2020-37222	Kuicms Php EE 2.0 contains a persistent cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted content through the bbs reply endpoint. Attackers can send POST requests to /web/?c=bbs&a=reply with HTML and JavaScript payloads in the content parameter to execute arbitrary scripts in users' browsers.	7.2	More Details
CVE-2026-8597	Missing integrity verification in the Triton inference handler in Amazon SageMaker Python SDK v2 before v2.257.2 and v3 before v3.8.0 might allow a remote authenticated actor to achieve code execution in inference containers via replacement of model artifacts in S3 with a specially crafted pickle payload that is deserialized without verification. This issue requires a remote authenticated actor with S3 write access to the model artifact path. To remediate this issue, we recommend upgrading to Amazon SageMaker Python SDK v2.257.2 or v3.8.0 and rebuild any Triton models previously created with ModelBuilder using the updated SDK.	7.2	More Details
	Cleartext storage of sensitive information in the ModelBuilder/Serve component in Amazon SageMaker Python SDK before v2.257.2 and v3 before v3.8.0 might allow a remote authenticated actor to extract the HMAC signing key from SageMaker API responses and forge		

CVE-2026-8596	valid integrity signatures for specially crafted model artifacts, achieving code execution in inference containers. This issue requires a remote authenticated actor with permissions to call SageMaker describe APIs and S3 write access to the model artifact path. To remediate this issue, we recommend upgrading to Amazon SageMaker Python SDK v2.257.2 or v3.8.0 and rebuild any models previously created with ModelBuilder using the updated SDK.	7.2	More Details
CVE-2026-45349	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, a user just needs to use the API endpoint: /api/chat/completions with their own API key (generated in OWUI) and the Chat ID of another user to continue the conversation of the other user. This vulnerability is fixed in 0.9.0.	7.1	More Details
CVE-2026-45399	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, any authenticated user with low privileges can enumerate active background tasks across the system and stop tasks belonging to other users via the GET /api/tasks and POST /api/tasks/stop/{task_id} methods. This allows a casual user to disrupt system-wide chat usage by continuously canceling other users' active tasks. This is a real authorization vulnerability affecting integrity and usability in multi-user deployments. This vulnerability is fixed in 0.9.0.	7.1	More Details
CVE-2021-47980	Fuel CMS 1.4.13 contains a blind SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'col' parameter in the Activity Log interface. Attackers can send requests to the logs endpoint with malicious SQL payloads in the 'col' parameter to extract database information based on response time delays.	7.1	More Details
CVE-2026-41935	Vvveb before 1.0.8.3 contains an uncontrolled recursion vulnerability in the admin controller dispatch cycle where Base::init() repeatedly invokes permission() on error handlers, causing infinite recursion until PHP memory limits are exhausted. Attackers can send sustained requests to forbidden admin URLs from a low-privilege account to exhaust PHP memory on all workers and cause denial of service to legitimate traffic.	7.1	More Details
CVE-2026-46446	SOGo before 5.12.7, when PostgreSQL or MariaDB is used, and cleartext passwords are stored, allows SQL injection. This is related to c_password = '%@' in changePasswordForLogin.	7.1	More Details
CVE-2026-44637	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. From to 1.8.7-r1, a signed integer overflow in the SIXEL parser's image-buffer doubling loop can lead to an out-of-bounds heap write in sixel_decode_raw_impl. context->pos_x grows by repeat_count on every sixel character with no upper bound check. Once pos_x approaches INT_MAX, the expression "pos_x + repeat_count" used to size the image buffer overflows signed int. Depending on how the overflow wraps, the resize check that should reject oversized buffers can be bypassed, after which a subsequent write computes a large attacker-influenced offset into image->data and writes past the allocation. Reachable from any caller that decodes attacker-supplied SIXEL data, including img2sixel. This vulnerability is fixed in 1.8.7-r2.	7.1	More Details
CVE-2026-46445	SOGo before 5.12.7, when PostgreSQL is used, allows SQL injection.	7.1	More Details
CVE-2018-25319	Redaxo CMS Addon MyEvents 2.2.1 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the myevents_id parameter. Attackers can send GET requests to the event_add.php page with malicious myevents_id values to extract or modify sensitive database information.	7.1	More Details
CVE-2026-44556	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the /responses endpoint in the OpenAI router accepts any authenticated user and forwards requests directly to upstream LLM providers without enforcing per-model access control. While the primary chat completion endpoint (generate_chat_completion) checks model ownership, group membership, and AccessGrants before allowing a request, the /responses proxy only validates that the user has a valid session via get_verified_user. This allows any authenticated user to interact with any model configured on the instance by sending a POST request to /api/openai/responses with an arbitrary model ID. This vulnerability is fixed in 0.9.0.	7.1	More Details
CVE-2026-32991	Improper authorization checks of team members privileges allow a team member to escalate privileges to the team owner account.	7.1	More Details
CVE-2026-32882	libheif is a HEIF and AVIF file format decoder and encoder. Versions 1.21.2 and prior contain a heap buffer over-read in HeifPixelImage::overlay() in libheif/pixelimage.cc. When compositing an overlay image (iovl) whose child image has a different bit depth for the alpha channel than for the color channels, the function indexes into the alpha plane using the color channel stride (in_stride) instead of the previously retrieved alpha_stride, causing reads past the end of the alpha buffer (up to 3,123 bytes for a 100×50 image with 10-bit color and 8-bit alpha). A crafted HEIF file can exploit this to cause a denial of service (crash) or potentially disclose adjacent heap memory through leaked bytes embedded in the decoded output pixels. This issue has been fixed in versionThis issue has been fixed in version 1.22.0.	7.1	More Details
CVE-2026-32741	libheif is a HEIF and AVIF file format decoder and encoder. Versions 1.21.2 and below contain a heap buffer overflow in MaskImageCodec::decode_mask_image(). When decoding a HEIF file containing a mask image (mski), the function copies the full iloc extent data into a pixel buffer using memcpy(dst, data.data(), data.size()). The copy length data.size() is determined by the iloc extent in the file (attacker-controlled), while the destination buffer is sized based on the declared image dimensions. Because no upper-bound check exists on the data length, a crafted file whose iloc extent exceeds the pixel buffer allocation overflows the heap. The vulnerable single-memcpy branch is reached when the mskC property specifies bits_per_pixel = 8 and the ispe property declares an even width ≥ 64 (so that stride == width), with no changes to default security limits or external codec plugins required. This issue has been fixed in version 1.22.0.	7.1	More Details
CVE-2026-4609	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the pm_invite_user function in all versions up to, and including, 5.9.8.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add themselves or any registered user to any ProfileGrid group, including closed and paid groups, bypassing all authorization and payment gates.	7.1	More Details
CVE-2026-45350	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.6, there is a vulnerability in chat completion API, which allows attackers to bypass tool restrictions, potentially enabling unauthorized actions or access. In the chat_completion API, the parameters tool_ids and tool_servers are supplied by the user. These parameters are used to create a tools_dict by the middleware. This is then used by get_tool_by_id to retrieve the appropriate tool. However, there is no checks in that ensures the user that uses the API has permission to use the tool, meaning that a user can invoke any server tool by supplying the correct tool_id or tool_servers parameters via the chat completion API. Moreover, the authentication token stored in the server would be used when invoking the tool, so the tool will be invoked with the server privilege. This vulnerability is fixed in 0.8.6.	7.1	More Details

CVE-2026-45242	Summarize prior to 0.15.1 contains a path traversal vulnerability in the /v1/summarize daemon endpoint that allows authenticated callers to write files to arbitrary directories by supplying an absolute path or directory traversal sequence in the slidesDir request parameter. Attackers can exploit this to write slide_*.png and slides.json files to any writable directory and subsequently delete matching files at the specified location through repeat extraction.	7.1	More Details
CVE-2026-7571	A flaw was found in Keycloak. A low-privilege user, with knowledge of user credentials and client ID, can bypass a security control intended to disable the implicit flow in OpenID Connect (OIDC) clients. By manipulating client data during a session restart, an attacker can obtain an access token that should not be available. This vulnerability can also lead to the exposure of these access tokens in server logs, proxy logs, and HTTP Referrer headers, resulting in sensitive information disclosure.	7.1	More Details
CVE-2026-44569	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.19, there's an IDOR in the channels message management system that allows authenticated users to modify or delete any message within channels they have read access to. The vulnerability exists in the message update and delete endpoints, which implement channel-level authorization but completely lack message ownership validation. While the frontend correctly implements ownership checks (showing edit/delete buttons only for message owners or admins), the backend APIs bypass these protections by only validating channel access permissions without verifying that the requesting user owns the target message. This creates a client-side security control bypass where attackers can directly call the APIs to modify other users' messages. This vulnerability is fixed in 0.6.19.	7.1	More Details
CVE-2026-33377	An Editor can overwrite a dashboard not owned by them to acquire admin on that specific dashboard. The user must have write access to the dashboard to escalate privilege.	7.1	More Details
CVE-2026-30950	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Versions 0.6.36 through 0.6.50 are vulnerable to Authenticated Session Hijacking via IDOR. If an authenticated attacker can determine the session_id of another user's session, they can take it over, reading any messages in it and locking the legitimate user out. The PATCH /sessions/{session_id}/assign-user endpoint authenticates the caller but never verifies session ownership: the service layer invokes the session lookup with user_id=None, which the data access layer interprets as a privileged/system call that bypasses the ownership filter, allowing any authenticated user to reassign an arbitrary session to themselves. This issue has been patched in version 0.6.51.	7.1	More Details
CVE-2026-44641	Microsoft APM is an open-source, community-driven dependency manager for AI agents. Prior to 0.8.12, Microsoft APM normalizes marketplace plugins by copying plugin components referenced in plugin.json into .apm/. The manifest fields agents, skills, commands, and hooks are attacker-controlled, but the implementation does not enforce that those paths remain inside the plugin directory. A malicious plugin can therefore use absolute paths or ../ traversal paths to copy arbitrary readable host files or directories from the installer's machine during apm install. This vulnerability is fixed in 0.8.12.	7.1	More Details
CVE-2020-37226	Joomla J2 JOBS 1.3.0 contains an authenticated SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'sortby' parameter. Attackers can send POST requests to the administrator index with malicious 'sortby' values to extract sensitive database information using automated tools.	7.1	More Details
CVE-2026-6495	The Ajax Load More WordPress plugin before 7.8.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	7.1	More Details
CVE-2020-37224	Joomla J2 JOBS 1.3.0 contains an authenticated SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'sortby' parameter. Attackers can send POST requests to the administrator index with malicious 'sortby' values to extract sensitive database information.	7.1	More Details
CVE-2026-45037	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.232, Tabby's terminal linkifier passes any detected URI directly to the operating system's protocol handler without validating the protocol scheme. This allows a malicious SSH or Telnet server to send crafted terminal output containing dangerous protocol URIs which Tabby renders as clickable links, triggering arbitrary OS protocol handlers on the victim's machine. This vulnerability is fixed in 1.0.232.	7.1	More Details
CVE-2026-45036	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.233, Tabby before 1.0.233 automatically confirms ZMODEM protocol detection on all terminal session output without user interaction, enabling shell command execution when a user displays attacker-controlled content. The ZModemMiddleware in tabby-terminal consumes all session output through a Zmodem.Sentry, and when a ZMODEM ZRQINIT header is detected, unconditionally calls detection.confirm() and writes a fixed ZRINIT response (**\x18B0100000023be50\r\n\x11) back into the active PTY as input. When the process that triggered the detection (e.g., cat) exits, the injected bytes are consumed by the user's shell as a command line. Under fish (default configuration), the ** prefix triggers recursive glob expansion against the current directory, allowing an attacker-placed executable at a matching nested path (e.g., d/xB0100000023be50) to be executed by relative pathname without relying on PATH. Under bash and zsh, a secondary xterm.js terminal color-query feedback (OSC 10) can be combined in the same file to inject a slash-containing command word that similarly bypasses PATH resolution. An attacker can exploit this by providing a crafted file (e.g., in a cloned Git repository) that a user displays with cat, achieving code execution with no interaction beyond viewing the file. This vulnerability is fixed in 1.0.233.	7.0	More Details
CVE-2026-46361	phpMyFAQ before 4.1.2 contains a stored cross-site scripting vulnerability in search.twig where result.question and result.answerPreview are rendered with the raw filter, disabling autoescape protection. Attackers with FAQ editor privileges can inject HTML-entity-encoded payloads that bypass html_entity_decode(strip_tags()) processing in SearchController.php, executing arbitrary JavaScript in every visitor's browser context including administrators.	6.9	More Details
CVE-2026-36742	Hiseeu C90 v5.7.15 is vulnerable to Insecure Permissions. The UART bootloader is accessible when battery is disconnected (hidden/debug mode).	6.8	More Details
CVE-2026-4630	A flaw was found in Keycloak. An authenticated client could exploit an Insecure Direct Object Reference (IDOR) vulnerability in the Authorization Services Protection API endpoint. By knowing or obtaining a resource's unique identifier (UUID) belonging to another Resource Server within the same realm, the client could bypass authorization checks. This allows the client to perform unauthorized GET, PUT, and DELETE operations on resources, leading to information disclosure and potential unauthorized modification or deletion of data.	6.8	More Details
CVE-2026-6008	Authorization bypass through User-Controlled key vulnerability in Im Park Information Technology, Electronics, Press, Publishing and Advertising, Education Ltd. Co. DijiDemi allows Privilege Abuse. This issue affects DijiDemi: from v4.5.12.1 before v4.5.13.0.	6.8	More Details
CVE-2026-41119	Dell Live Optics Windows and Personal Edition collectors contain an improper certificate validation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability leading to loss of confidentiality and integrity.	6.8	More Details

CVE-2026-42586	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, the Netty Redis codec encoder (RedisEncoder) writes user-controlled string content directly to the network output buffer without validating or sanitizing CRLF (\r\n) characters. Since the Redis Serialization Protocol (RESP) uses CRLF as the command/response delimiter, an attacker who can control the content of a Redis message can inject arbitrary Redis commands or forge fake responses. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	6.8	More Details
CVE-2026-21021	Improper input validation in Routines prior to SMR May-2026 Release 1 allows physical attackers to launch privileged activity.	6.8	More Details
CVE-2026-36738	U-SPEED AC1200 Gigabit Wi-Fi Router (Model: T18-21K) V1.0 is vulnerable to Incorrect Access Control. The device exposes a UART interface that lacks authentication, authorization, or access control mechanisms. An attacker with physical access to the UART pins can connect to the interface and gain unrestricted access to device functionality.	6.8	More Details
CVE-2026-41970	Out-of-bounds write vulnerability in the distributed file system module. Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2026-33741	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below allow authenticated users to upload SVG attachments through normal attachment-capable fields and later serve those SVG files as top-level inline documents through both the attachment and image entry points, resulting in stored cross-user XSS reachable through a normal attachment workflow. Although inline SVG script is blocked by the response CSP, the same CSP still allows same-origin external script. As a result, an attacker can upload a malicious SVG together with a second attacker-controlled JavaScript attachment, then trick another user into opening the SVG to execute JavaScript in the victim's EspoCRM origin. This issue has been fixed in version 9.3.4.	6.8	More Details
CVE-2026-1322	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.0 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with a read_api scoped OAuth application to create issues and add comments to issues in private projects due to improper authorization.	6.8	More Details
CVE-2026-24464	When running in Appliance mode, a directory traversal vulnerability exists in an undisclosed iControl REST endpoint that may allow an authenticated attacker with administrator role privileges to cross a security boundary and delete files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.8	More Details
CVE-2026-37982	A flaw was found in Keycloak. This authentication vulnerability allows a remote attacker to replay `ExecuteActionsActionToken` tokens within Keycloak's WebAuthn (Web Authentication) flow. By intercepting an execute-actions email link, an attacker can register their own authenticator to a victim's account. This leads to unauthorized enrollment of a hardware-backed credential, enabling persistent account takeover.	6.8	More Details
CVE-2026-21018	Out-of-bounds write in SveService prior to SMR May-2026 Release 1 allows local privileged attackers to execute arbitrary code.	6.7	More Details
CVE-2026-42919	A vulnerability exists in BIG-IP systems that may allow an authenticated attacker with administrative access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.7	More Details
CVE-2026-34216	CtrlPanel is open-source billing software for hosting providers. In versions 1.1.1 and prior, the admin settings update endpoint accepted a fully qualified class name directly from user-supplied request input and used it for dynamic static method calls and object instantiation without any allowlist validation, allowing for authenticated Remote Code Execution. An authenticated admin-level user could supply an arbitrary class name available in the Composer autoloader, potentially triggering unintended constructor or magic method execution. The update() method reads settings_class directly from the HTTP request and passed it to new $settings_class() and $settings_class::getValidations() without verifying that the provided value corresponds to a legitimate settings class: Because PHP resolves class names against the Composer autoloader at runtime, any autoloadable class in the application or its dependencies could be instantiated. Depending on the classes available in the dependency tree, this can trigger unintended side effects through constructors or magic methods (__construct, __toString, __wakeup), following a PHP object injection / gadget chain pattern. This issue has been fixed in version 1.2.0.	6.6	More Details
CVE-2026-41959	Incorrect permission assignment vulnerabilities exist in BIG-IP and BIG-IQ TMOS Shell (tmsh) network diagnostics commands and in BIG-IP iControl REST. These vulnerabilities may allow an authenticated attacker to view the network status of destination systems. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-45773	Turborepo is a high-performance build system for JavaScript and TypeScript codebases. Prior to 2.9.14, Turborepo's self-hosted login and SSO browser flows did not validate a CSRF state value on the localhost callback. While the CLI was waiting for authentication, a malicious web page could send a request to the local callback server with an attacker-controlled token. If accepted before the legitimate callback, the CLI could complete login with the wrong credentials. This affects users authenticating the turbo CLI against self-hosted remote cache/auth endpoints. Vercel-hosted login flows using device authorization are not affected. This vulnerability is fixed in 2.9.14.	6.5	More Details
CVE-2026-8503	Apache::Session::Generate::SHA256 versions before 1.3.19 for Perl create insecure session ids. Apache::Session::Generate::SHA256 generated session ids insecurely. The default session id generator returns a SHA-256 hash of the built-in rand() function, the epoch time, and the PID, that is hashed again. These are predictable, low-entropy sources. Predicable session ids could allow an attacker to gain access to systems. Note that version 1.3.19 has a fallback without warning to use insecure session generation method if the call to Crypt::URandom::urandom fails. However, this is unlikely as Crypt::URandom is a hardcoded requirement of the module. This issue is similar to CVE-2025-40931 for Apache::Session::Generate::MD5.	6.5	More Details
CVE-2026-39052	Oinone Pamirs 7.0.0 contains a code execution vulnerability via ScriptRunner. The method ScriptRunner.run(String expression, String type, Map<String, Object> context) evaluates attacker-controlled script expressions through the underlying script engine without sandboxing or allowlist restrictions.	6.5	More Details
CVE-2023-7345	Ledger Live with vulnerable versions of ledgerhq/hw-app-eth prior to 6.34.7 contains an integer parsing vulnerability that allows attackers to manipulate EIP-712 typed data messages by exploiting incorrect hexadecimal field parsing when values contain an odd number of characters. Attackers can obtain signatures on truncated or misinterpreted message values to authorize unintended blockchain transactions, such as asset transfers at incorrect amounts.	6.5	More Details
CVE-2026-8669	Imager versions through 1.030 for Perl allow a heap out of bounds (OOB) write on crafted multi-frame GIF files. Imager::File::GIF's i_readgif_multi_low allocates a single per-row buffer GifRow sized for the GIF's global screen width 'SWidth' and reuses it across every image in the file. The page-match branch validates Image.Width + Image.Left > SWidth before each DGifGetLine write, but the parallel skip-image branch at imgif.c:790-805 calls DGifGetLine(GifFile, GifRow, Width) with no such check.	6.5	More Details

CVE-2026-45339	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, Open WebUI allows admins to restrict which API endpoints an API key can access. When an API key is restricted from /api/v1/messages, requests using the Authorization: Bearer sk-... header are correctly blocked with 403. However, the same key sent via the x-api-key header bypasses the restriction entirely — the request is authenticated, the model is invoked, and a full response is returned. This vulnerability is fixed in 0.9.0.	6.5	More Details
CVE-2026-8738	A security vulnerability has been detected in Sanluan PublicCMS 5.202506.d. Impacted is the function TradeOrderController.pay/TradePaymentController.pay/AccountGatewayComponent.pay of the file publiccms-trade/src/main/java/com/publiccms/controller/web/trade/TradeOrderController.java of the component Trade Payment Flow. The manipulation leads to business logic errors. Remote exploitation of the attack is possible. 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.	6.5	More Details
CVE-2026-26062	Fleet is open source device management software. Prior to version 4.81.0, Fleet contained a denial-of-service (DoS) issue in the gRPC Launcher `PublishLogs` endpoint. In affected versions, certain unexpected input values were not handled gracefully, which could cause the Fleet server process to terminate while processing an authenticated request from an enrolled Launcher host. An authenticated attacker with access to any enrolled Launcher node key could cause an immediate and complete denial of service by sending a single gRPC request to the `PublishLogs` endpoint. This vulnerability impacts availability only. There is no exposure of sensitive data, no authentication bypass, no privilege escalation, and no integrity impact. Version 4.81.0 contains a patch. If upgrading immediately is not possible, the following mitigations can reduce exposure. Restrict network access to the Fleet gRPC endpoint where feasible (for example, limiting inbound access to known host IP ranges); deploy Fleet behind infrastructure that terminates or filters gRPC traffic if Launcher log ingestion is not required; and/or monitor for repeated Fleet process crashes or unexpected restarts indicating potential exploitation.	6.5	More Details
CVE-2026-42781	When embedded Packet Velocity Acceleration (ePVA) acceleration is configured, undisclosed local ethernet traffic can cause an increase in ePVA and Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-8570	Type Confusion in V8 in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-27737	BigBlueButton is an open-source virtual classroom. In versions prior to 3.0.19, the recording playback (presentation format) was not sanitizing user's input in public chat. This allowed for a malicious actor to craft and carry out a targeted XSS attack, activated on anyone replaying the recording. This issue has been fixed 3.0.19.	6.5	More Details
CVE-2026-44562	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the POST /api/v1/models/import endpoint allows users with the workspace.models_import permission to overwrite any existing model in the database, regardless of ownership. When an imported model's ID matches an existing model, the endpoint merges the attacker's payload over the existing model data and writes it to the database with no ownership or access grant validation. Additionally, filter_allowed_access_grants is never called, bypassing the access grant restrictions enforced on all other model mutation endpoints. This vulnerability is fixed in 0.9.0.	6.5	More Details
CVE-2026-46719	Net::Statsd::Lite versions before 0.9.0 for Perl allowed metric injections. The metric names were not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics.	6.5	More Details
CVE-2025-67437	Medical Management System a81df1ce700a9662cb136b27af47f4cbde64156b is vulnerable to Insecure Permissions, which allows arbitrary user password reset.	6.5	More Details
CVE-2026-4608	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to blind SQL Injection via the 'rid' parameter in all versions up to, and including, 5.9.8.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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-2026-44560	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the type: "file" (non-full-context), type: "text" with collection_name, and bare collection_name/collection_names paths in the get_sources_from_items function perform vector store queries without any authorization check, allowing users to extract content from files and knowledge bases they do not have access to. This vulnerability is fixed in 0.9.0.	6.5	More Details
CVE-2026-35086	Improper Control of Generation of Code ('Code Injection') vulnerability in email services of Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.5	More Details
CVE-2026-44571	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.6, in standard channels (i.e., channels whose channel.type is neither group nor dm), the endpoint POST /api/v1/channels/{channel_id}/messages/{message_id}/update can be accessed with read permission only. When access_control is set to None, the authorization check has_access(..., type="read") evaluates to True, allowing users who are not the message owner to update messages. As a result, unauthorized modification of other users' messages is possible. This vulnerability is fixed in 0.8.6.	6.5	More Details
CVE-2026-28733	in OpenHarmony v6.0 and prior versions allow a local attacker arbitrary code execution.	6.5	More Details
CVE-2026-4782	The Avada Builder plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 3.15.2 via the 'fusion_get_svg_from_file' function with the 'custom_svg' parameter of the 'fusion_section_separator' shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The vulnerability was partially patched in version 3.15.2 and fully patched in version 3.15.3.	6.5	More Details
CVE-2026-45008	phpMyFAQ before 4.1.2 contains a path traversal vulnerability in Client::deleteClientFolder that allows admins with INSTANCE_DELETE permission to delete arbitrary directories. Attackers can submit traversal sequences like https://../../../<path> in the client URL parameter to recursively delete directories outside the intended clientFolder scope.	6.5	More Details
CVE-2026-37428	qihang-wms commit 75c15a was discovered to contain a SQL injection vulnerability via the datascope parameter in the SysDeptMapper.xml file. This vulnerability allows attackers to access sensitive database information, including users' Personally Identifiable Information (PII).	6.5	More Details

CVE-2026-45667	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, GET /api/v1/memories/ef is accessible without authentication and executes request.app.state.EMBEDDING_FUNCTION(...). This allows any unauthenticated caller to trigger embedding generation which can lead to direct cost exposure if a paid provider is used. This vulnerability is fixed in 0.8.0.	6.5	More Details
CVE-2026-8550	Use after free in Google Lens in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-31156	A path injection vulnerability exists in OpenPLC v3 (2c82b0e79c53f8c1f1458eee15fec173400d6e1a) as the binary program compiled from glue_generator.cpp does not perform any validation on the file path parameters passed via the command line. The user-controlled input parameters are directly passed to the underlying file operation functions (fopen/ifstream/ofstream) for file reading and writing. An attacker can exploit this vulnerability by constructing a malicious path to read arbitrary readable files.	6.5	More Details
CVE-2026-29207	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue. Please note that in the updated version, "Data Resource" records with dataTemplateTypeId = "FTL" are no longer supported. Additionally, in the updated version, the "Ecommerce Customer" security group no longer includes content management grants. Users are advised to remove these permissions from any production site as well.	6.5	More Details
CVE-2026-29220	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.5	More Details
CVE-2026-37979	A flaw was found in Keycloak. This access control vulnerability in Keycloak's OpenID Connect (OIDC) token introspection endpoint allows a confidential client to bypass audience restrictions. An attacker-controlled client with valid credentials can retrieve sensitive token claims intended for other resource servers, compromising the confidentiality of lightweight access tokens. This issue can be exploited remotely by any confidential client in the realm with valid credentials.	6.5	More Details
CVE-2026-45666	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.11, the API /api/v1/notes/{note_id} endpoint lacks proper authorization checks, allowing authenticated users to retrieve notes belonging to other users by guessing or enumerating UUIDs. This results in unauthorized disclosure of potentially sensitive or private user data. This vulnerability is fixed in 0.8.11.	6.5	More Details
CVE-2026-34233	CtrlPanel is open-source billing software for hosting providers. In versions 1.1.1 and prior, multiple admin controllers expose DataTable endpoints without authorization checks, allowing any authenticated user to access sensitive administrative data that should be restricted to administrators only. The affected admin controllers define datatable() methods that are reachable via GET requests but lack any permission or role verification. Because the routes fall under the /admin/ prefix, operators may assume they are protected - however, the middleware applied to this route group does not enforce admin-level authorization on these specific endpoints. As a result, any authenticated user (regardless of role) can query these endpoints and receive paginated JSON responses containing sensitive records. Exploitation can result in enumeration of user PII, payment and transaction records, active voucher and coupon codes, role and permission structure, server ownership mappings and support ticket contents. This issue has been fixed in version 1.2.0.	6.5	More Details
CVE-2026-35062	An authenticated iControl SOAP user may be able to obtain information of other accounts. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-45351	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.9, when a regular user [non-admin] logs into the application, a http://IP:8080/api/models? web request is initiated by the application and in response, it reveals the system prompt of available models set by admin on models pages in workspace affecting the confidentiality of application. This vulnerability is fixed in 0.8.9.	6.5	More Details
CVE-2026-45345	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.5.7, a user can modify another user's model even if its visibility is set to Private. By changing the access permissions during editing, unauthorized access can be gained. This vulnerability is fixed in 0.5.7.	6.5	More Details
CVE-2026-8704	Crypt::DSA versions through 1.19 for Perl use 2-args open, allowing existing files to be modified.	6.5	More Details
CVE-2026-31378	Improper Input Validation vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.5	More Details
CVE-2026-4683	The Smartcat Translator for WPML plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'routeData' REST endpoint in all versions up to, and including, 3.1.77. This makes it possible for unauthenticated attackers to overwrite the plugin's Smartcat API credentials (account ID, API secret key, hub key, API host, and hub host), effectively hijacking the translation service or causing a denial of service.	6.5	More Details
CVE-2026-46362	phpMyFAQ before 4.1.2 contains an authorization bypass vulnerability in AbstractAdministrationController::userHasPermission() that fails to terminate execution after sending a forbidden response. Attackers can access all permission-protected admin pages by requesting their URLs as authenticated users, exposing admin logs, user data, system information, and application configuration.	6.5	More Details
CVE-2026-5545	libcurl might in some circumstances reuse the wrong connection when asked to do an authenticated HTTP(S) request after a Negotiate-authenticated one, when both use the same host. libcurl features a pool of recent connections so that subsequent requests can reuse an existing connection to avoid overhead. When reusing a connection a range of criteria must be met. Due to a logical error in the code, a request that was issued by an application could wrongfully reuse an existing connection to the same server that was authenticated using different credentials. An application that first uses Negotiate authentication to a server with `user1:password1` and then does another operation to the same server asking for any authentication method but for `user2:password2` (while the previous connection is still alive) - the second request gets confused and wrongly reuses the same connection and sends the new request over that connection thinking it uses a mix of user1's and user2's credentials when it is in fact still using the connection authenticated for user1...	6.5	More Details
CVE-2026-39053	Oinone Pamirs 7.0.0 contains an XML External Entity (XXE) issue in its XStream-based XML parsing logic. When attacker-controlled XML is passed to framework parsing entry points such as PamirsXmlUtils.fromXML(...) or ViewXmlUtils.fromXML(...), unsafe XML processing can lead to file disclosure or SSRF.	6.5	More Details
CVE-	When NGINX Plus or NGINX Open Source are configured to use the HTTP/3 QUIC module, an attacker may be able to spoof their source IP		More

2026-40460	address allowing for bypass of authorization or bypass of rate limiting. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	Details
CVE-2026-40462	Incorrect permission assignment vulnerabilities exist in iControl REST and TMOS shell (tmsh) undisclosed command which may allow an authenticated attacker to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-31380	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.5	More Details
CVE-2026-40699	A vulnerability exists in the undisclosed pages in the Configuration utility that may allow a low-privileged authenticated attacker to access to undisclosed sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-41219	An improper sanitization vulnerability exists in the BIG-IP QKView utility that allows a low-privileged attacker to read sensitive information from a QKView file. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.5	More Details
CVE-2026-45187	Improper Authorization vulnerability in Apache OFBiz Webtools. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.5	More Details
CVE-2026-37429	qihang-wms commit 75c15a was discovered to contain a SQL injection vulnerability via the datascope parameter in the SysUserMapper.xml file. This vulnerability allows attackers to access sensitive database information, including users' Personally Identifiable Information (PII) via a crafted SQL statement.	6.5	More Details
CVE-2026-44000	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, a sandbox boundary violation in vm2 allows host object identity to cross into the sandbox through host Promise resolution. When a host-side Promise that resolves to a host object is exposed to the sandbox, the value delivered to the sandbox .then() callback preserves host identity. This allows the sandbox to interact with the host object directly, including performing identity checks using host-side WeakMap and mutating host object state from inside the sandbox. This behavior occurs because the Promise fulfillment wrapper uses ensureThis() instead of the stronger cross-realm conversion path (from() / proxy wrapping). If no prototype mapping is found, ensureThis() returns the original object. As a result, objects resolved by host Promises can cross the sandbox boundary without proper isolation. This vulnerability is fixed in 3.11.0.	6.5	More Details
CVE-2026-3471	Mattermost Desktop App versions <=6.1 6.0.1 5.4.13.0 fail to prevent an invalid URL from loading in a pop-up window in the Mattermost Desktop App which allows a malicious server owner to repeated crash the application via calling {{window.open('javascript:alert()');}}. Mattermost Advisory ID: MMSA-2026-00618	6.5	More Details
CVE-2026-32814	libheif is a HEIF and AVIF file format decoder and encoder. In versions 1.21.2 and prior, when decoding a HEIF grid image with strict_decoding=false (the default), a corrupted tile silently fails to decode and the library returns heif_error_Ok with no indication of failure, leading to an uninitialized heap memory information leak. The canvas is allocated via create_clone_image_at_new_size() → plane.alloc() → new (std::nothrow) uint8_t[allocation_size] which does not zero the memory; only the alpha plane is explicitly initialized via fill_plane(), so the Y, Cb, and Cr planes contain whatever was previously at that heap address. The failed tile's region of the canvas is never written. It retains uninitialized heap data that is delivered to the caller as decoded pixel values (4,096 bytes per Y/Cb/Cr plane = 12,288+ bytes total). Any application using libheif to decode grid-based HEIF/AVIF files with default settings is vulnerable: a crafted .heic or .avif file causes 4,096+ bytes of heap memory to appear as pixel values in the decoded image, and the calling application receives heif_error_Ok, so it has no indication the output contains heap garbage. In server-side image processing, an uploaded crafted HEIF decoded and re-encoded (e.g., as PNG/JPEG for thumbnails, CDN, social media) can leak cross-user data such as auth tokens, database results, and other users' image data. This issue has been fixed in version 1.22.0.	6.5	More Details
CVE-2026-8843	Creating a "2dsphere_bucket" index on a non-timeseries bucket collection will succeed, but any subsequent attempt to insert a document which triggers updating that index will crash the server. A similar issue occurs when creating "queryable_encrypted_range" indices. This issue affects MongoDB Server v7.0 versions prior to 7.0.32, v8.0 versions prior to 8.0.21 and v8.2 versions prior to 8.2.6	6.5	More Details
CVE-2026-8199	An authenticated user can cause excess memory usage via bitwise match expression AST processing of $bitsAllSet, $bitsAnySet, $bitsAllClear, and $bitsAnyClear. This contributes to memory pressure and may lead to availability loss by OOM. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	6.5	More Details
CVE-2026-5486	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to SQL Injection via the 'data[filter_search]' parameter in the get_cat_addons AJAX action in versions up to and including 2.0.7. This is due to insufficient input sanitization and the use of deprecated escaping functions combined with direct string concatenation in SQL query construction. The vulnerability is exacerbated because the normalizeAjaxInputData() function calls stripslashes() on all user input, removing the protection provided by WordPress's wp_magic_quotes() function. Subsequently, the filter_search parameter is escaped using the deprecated wpdb->_escape() function and then directly concatenated into a LIKE clause without using prepared statements. This makes it possible for authenticated attackers, with Contributor-level access and above (who can obtain a valid nonce through the Elementor editor), to inject arbitrary SQL commands and extract sensitive information from the database.	6.5	More Details
CVE-2026-8972	Privilege escalation in the WebRTC: Audio/Video component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	6.5	More Details
CVE-2026-6345	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail prevent disclosure of created user password which allows a malicious attacker to impersonate a user via the use of some of those passwords.. Mattermost Advisory ID: MMSA-2026-00614	6.5	More Details
CVE-2026-1184	GitLab has remediated an issue in GitLab EE affecting all versions from 11.9 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to cause denial of service by uploading a specially crafted file due to improper validation.	6.5	More Details
CVE-2026-5163	Mattermost versions 11.5.x <= 11.5.1 fail to verify channel membership when processing AI-assisted message rewrites which allows an authenticated attacker to read the content of threads in private channels and direct messages they do not have access to via a crafted request to the post rewrite endpoint.. Mattermost Advisory ID: MMSA-2026-00645	6.5	More Details
CVE-	A Stored HTML Injection vulnerability was discovered in the Smart Polling functionality due to improper validation of an input parameter. An authenticated user with limited privileges can push malicious remote strategies containing HTML tags through the sync. When a		More

2025-40904	victim views the affected remote strategy in the Smart Polling functionality, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	6.5	Details
CVE-2026-23557	Any guest can cause xenstored to crash by issuing a XS_RESET_WATCHES command within a transaction due to an assert() triggering. In case xenstored was built with NDEBUG #defined nothing bad will happen, as assert() is doing nothing in this case. Note that the default is not to define NDEBUG for xenstored builds even in release builds of Xen.	6.5	More Details
CVE-2026-3117	Mattermost Plugins versions <=11.5 11.1.5 10.13.11 11.3.4.0 fail to properly check for permissions when processing commands in the Gitlab plugin which allows normal users to uninstall instances or setup webhook connections via the {{gitlab instance {option}}} or the {{/gitlab webhook {option}}} commands. Mattermost Advisory ID: MMSA-2026-00600	6.5	More Details
CVE-2026-4524	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.9.1 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to access confidential issue content in public projects without proper authorization due to improper authorization checks.	6.5	More Details
CVE-2026-8706	Firefox for iOS hosted Reader mode on an unauthenticated local web server, allowing another application on the same device to request arbitrary URLs and receive the response rendered with the signed-in user's cookies. This vulnerability was fixed in Firefox for iOS 151.0.	6.5	More Details
CVE-2026-4527	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.10 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to create unauthorized Jira subscriptions for a targeted user's namespace via a specially crafted link due to missing CSRF protection.	6.5	More Details
CVE-2026-44456	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.16, bodyLimit() does not reliably enforce maxSize for requests without a usable Content-Length (e.g. Transfer-Encoding: chunked). Oversized requests can reach handlers and return 200 instead of 413. This vulnerability is fixed in 4.12.16.	6.5	More Details
CVE-2026-32739	libheif is a HEIF and AVIF file format decoder and encoder. In versions 1.21.2 and below, a crafted 800-byte HEIF sequence file causes an infinite loop in Box_stts::get_sample_duration(), consuming 100% CPU indefinitely with zero progress, leading to DoS. The loop has no iteration limit or timeout and is triggered during file open (parsing) - before any user interaction or image decoding. The process stays alive (no crash, no error logged), making it invisible to crash-based monitoring. This issue has been fixed in version 1.22.0.	6.5	More Details
CVE-2026-42585	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, Netty incorrectly parses malformed Transfer-Encoding, enabling request smuggling attacks. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	6.5	More Details
CVE-2026-8280	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.3 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to cause denial of service through excessive memory consumption due to improper input validation.	6.5	More Details
CVE-2026-8096	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.0.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to view all Kirki frontend forms and read stored visitor form submission data, including contact details, messages, and any other visitor-provided information submitted through site forms.	6.5	More Details
CVE-2026-42580	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, Netty's chunk size parser silently overflows int, enabling request smuggling attacks. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	6.5	More Details
CVE-2026-5193	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 6.5.13. This is due to insufficient role validation in the 'register_user' function, which only blocks the 'administrator' role. This makes it possible for authenticated attackers, with author level access and above, to create new user accounts with elevated privileges such as editor.	6.5	More Details
CVE-2026-6478	Covert timing channel in comparison of MD5-hashed password in PostgreSQL authentication allows an attacker to recover user credentials sufficient to authenticate. This does not affect scram-sha-256 passwords, the default in all supported releases. However, current databases may have MD5-hashed passwords originating in upgrades from PostgreSQL 13 or earlier. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	6.5	More Details
CVE-2026-6225	The Taskbuilder – Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'project_search' parameter in all versions up to, and including, 5.0.6 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 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-2026-6670	The Media Sync plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.4.9 via the 'sub_dir' and 'media_items' parameters. This is due to insufficient validation of user-supplied file paths, which are not checked for directory traversal sequences or restricted to the intended uploads directory. This makes it possible for authenticated attackers, with Author-level access and above, to perform actions on files outside of the originally intended directory.	6.5	More Details
CVE-2026-8951	Spoofing issue in the Toolbar component in Firefox for Android. This vulnerability was fixed in Firefox 151.	6.5	More Details
CVE-2026-22677	Hermes WebUI prior to 0.51.44 - Release T contains a path traversal vulnerability in the session import endpoint that allows authenticated attackers to read arbitrary files by importing a crafted session with an unrestricted workspace value. Attackers can supply a blocked filesystem root in the workspace field and subsequently use relative paths in the session file API to access any file readable by the WebUI process.	6.5	More Details
CVE-2026-8952	Privilege escalation in the Application Update component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	6.5	More Details
CVE-	Privilege escalation in the DOM: Workers component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151,		More

2026-8955	and Thunderbird 140.11.	6.5	Details
CVE-2026-28376	The Grafana Live push endpoint can be exploited to cause unbounded memory allocation by sending a large or streaming request body, potentially leading to out-of-memory conditions. An authenticated user with access to the Grafana Live API can trigger this issue.	6.5	More Details
CVE-2026-8957	Privilege escalation in the Enterprise Policies component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	6.5	More Details
CVE-2026-28383	A request to the Grafana plugin resources endpoint can cause unbounded memory allocation by reading the entire request body into memory. An authenticated user can exploit this to trigger an out-of-memory condition, potentially causing a denial of service.	6.5	More Details
CVE-2026-8971	Same-origin policy bypass in the Networking: JAR component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	6.5	More Details
CVE-2026-33378	Using the $__timeGroup macro, one can achieve an OOM by overloading the server. This requires a SQL datasource. If the server is set up to auto-restart, the impact is minimal or non-existent, as the attack can take upwards of half an hour to crash the server.	6.5	More Details
CVE-2026-27892	FacturaScripts is an open source accounting and invoicing software. In versions prior to 2026, the Library module stores and serves uploaded images byte-for-byte, without stripping EXIF/XMP/IPTC metadata. Any authenticated user who downloaded an image could extract the uploader's embedded metadata, which included GPS coordinates, device information, timestamps, embedded comments/notes, thumbnail previews, and other personally identifiable information (PII) preserved in the image metadata. Of all FacturaScripts' image upload features, only the Library module combined unrestricted uploads, persistent storage, authenticated download access, and a total lack of server-side metadata sanitization. This vulnerability carries significant real-world impact: an employee uploading a photo taken at their home inadvertently discloses their precise home address to every user with Library download access. This issue has been fixed in version 2026.	6.5	More Details
CVE-2026-41888	Distribution is a toolkit to pack, ship, store, and deliver container content. Prior to 3.1.1, tag deletion via the DELETE /v2/<name>/manifests/<tag> endpoint bypasses the storage.delete.enabled: false configuration, allowing any API client to remove tags from repositories even when the operator has explicitly disabled deletion. This vulnerability is fixed in 3.1.1.	6.5	More Details
CVE-2026-44424	ShellHub is a centralized SSH gateway. Prior to 0.24.2, GET /api/devices/:uid returns the full device object whenever the caller is authenticated, without verifying that the device belongs to the caller's namespace (tenant). Any authenticated user (JWT or API Key) who knows or can guess a device UID can read device metadata from any other namespace. This vulnerability is fixed in 0.24.2.	6.5	More Details
CVE-2026-44426	ShellHub is a centralized SSH gateway. Prior to 0.24.2, GET /api/namespaces/:tenant returns the full namespace object — including the members list (user IDs, e-mails, roles), settings, and device counts — to any caller authenticated by an API Key, for any tenant, regardless of the API Key's own tenant scope. The handler conditionally skips the membership check when the user ID (X-ID) is absent, which is exactly the case for API Key authentication. This vulnerability is fixed in 0.24.2.	6.5	More Details
CVE-2026-44440	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.101.1 and 16.10.0, an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability on an endpoint allows an authenticated adjacent attacker to read arbitrary files. This vulnerability is fixed in 15.101.1 and 16.10.0.	6.5	More Details
CVE-2026-7619	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 1.8.10.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with access to the donation management admin area (requiring the edit_others_donations capability) 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-2026-28379	A race condition in Grafana Live allows authenticated users with Viewer role to trigger a server crash by sending concurrent requests that cause a fatal map access error. This results in complete service unavailability requiring restart of the Grafana server.	6.5	More Details
CVE-2026-28380	Any Editor could delete any snapshot, even if they have no access to read or write them.	6.5	More Details
CVE-2026-44445	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.104.3 and 16.12.0, an improper restriction of XML external entity (XXE) reference vulnerability in the EDI Module enables an authenticated attacker to read files from the local file system, including sensitive configuration files. This vulnerability is fixed in 15.104.3 and 16.12.0.	6.5	More Details
CVE-2026-44423	ShellHub is a centralized SSH gateway. Prior to 0.24.2, GET /api/sessions/:uid returns the full session object for any authenticated caller, without scoping by the caller's tenant. An authenticated user can read session records (SSH username, device UID, remote IP, terminal type, authenticated flag, timestamps) belonging to any other namespace. This vulnerability is fixed in 0.24.2.	6.5	More Details
CVE-2026-42937	Incorrect permission assignment vulnerabilities exist in BIG-IP and BIG-IQ TMOS Shell (tmsh) arp and ndp commands, and in BIG-IP iControl REST. These vulnerabilities may allow an authenticated attacker to view adjacent network information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-42946	A vulnerability exists in the ngx_http_scgi_module and ngx_http_uwsgi_module modules that may result in excessive memory allocation or an over-read of data. When scgi_pass or uwsgi_pass is configured, an unauthenticated attacker with man-in-the-middle (MITM) ability to control responses from an upstream server may be able to read the memory of the NGINX worker process or restart it. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2026-20685	An attacker in a privileged network position may be able to leak sensitive information. A path handling issue was addressed with improved validation. This issue is fixed in PCC Release 5E290.3.	6.5	More Details
CVE-	Kubetail is a real-time logging dashboard for Kubernetes. Prior to 0.14.0, Kubetail's dashboard exposes WebSocket endpoints that did not adequately validate the Origin header on connection upgrade. A malicious web page visited by a user with an active Kubetail session		More

2026-44514	could open a WebSocket to the user's dashboard and read their Kubernetes logs in real time. This is a Cross-Site WebSocket Hijacking (CSWSH) vulnerability and affects both the desktop deployment (default http://localhost:7500) and cluster deployments (typically behind an Ingress with HTTP basic auth). This vulnerability is fixed in 0.14.0.	6.5	Details
CVE-2026-32738	libheif is a HEIF and AVIF file format decoder and encoder. In versions 1.21.2 and below, a crafted 792-byte HEIF sequence file with samples_per_chunk=0 in the stsc box causes an unsigned integer underflow in the Chunk constructor (m_last_sample = 0 + 0 - 1 = UINT32_MAX), mapping all samples to an empty chunk and resulting in a denial of service. When any sample is accessed, the library reads from index 0 of an empty std::vector, causing a guaranteed SEGV (null-page read). The file parses successfully without producing an error; the crash occurs on the first frame access. This issue has been fixed in version 1.22.0.	6.5	More Details
CVE-2026-22706	Strapi is an open source headless content management system. In Strapi versions prior to 5.33.3, changing or resetting a user's password did not invalidate the user's existing refresh-token sessions by default. The refresh-token invalidation step in the users-permissions and admin authentication controllers was conditional on a caller-supplied `deviceId`. When a password change or reset request did not include a `deviceId`, no refresh tokens were revoked, leaving every prior session active. An attacker who had previously obtained a refresh token could continue minting new access tokens after the legitimate user reset their password, allowing persistent unauthorized access for the lifetime of the refresh token (up to 30 days by default). Rotating credentials no longer terminated an active attacker session, defeating password reset as a containment measure. The patch in version 5.33.3 invalidates all refresh tokens associated with the user on every password change and password reset, regardless of whether a `deviceId` is supplied. A new device-scoped session is then issued to the caller as part of the response.	6.5	More Details
CVE-2020-37233	WordPress Plugin Buddypress 6.2.0 contains a persistent cross-site scripting vulnerability that allows authenticated attackers with moderator privileges to inject malicious script code through the figure parameter in wp:html blocks. Attackers can inject iframe elements with event handlers like onload that execute when administrators or privileged users preview or view the affected page content, enabling session hijacking and persistent phishing attacks.	6.4	More Details
CVE-2026-6504	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title_tag' parameter in all versions up to, and including, 1.7.1058 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-2026-3694	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' attribute of the bt_bb_button shortcode in all versions up to, and including, 5.6.8. 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-2020-37235	WordPress Theme Wibar 1.1.8 contains a stored cross-site scripting vulnerability in the Brand component that allows authenticated users to inject malicious scripts by manipulating the Logo URL parameter. Attackers with editor, administrator, contributor, or author privileges can inject base64-encoded script payloads through the ftc_brand_url input field to execute arbitrary JavaScript when users visit the brand page.	6.4	More Details
CVE-2020-37237	Composr CMS 10.0.34 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through the banner management interface. Attackers with admin credentials can inject XSS payloads in the Description field of the Add banner functionality, which execute for all website visitors when they access the home page.	6.4	More Details
CVE-2020-37236	NewsLister contains an authenticated persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through the title parameter in the news addition interface. Attackers can inject JavaScript payloads via the title field in the admin panel that execute when news items are viewed by other users.	6.4	More Details
CVE-2020-37225	Powie's WHOIS Domain Check 0.9.31 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary JavaScript by exploiting unsanitized input fields in plugin settings. Attackers can submit malicious payloads through textarea and input elements in the pwhois_settings.php configuration page to execute JavaScript in the admin context and escalate privileges.	6.4	More Details
CVE-2020-37238	CMS Made Simple 2.2.15 contains a stored cross-site scripting vulnerability that allows authenticated users with Content Manager access to inject malicious scripts through SVG file uploads. Attackers can upload SVG files containing embedded JavaScript to the file manager, which executes when other authenticated users access the uploaded file, enabling cookie theft and session hijacking.	6.4	More Details
CVE-2021-47957	Cookie Law Bar 1.2.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting unsanitized input to the Bar Message field. Attackers can inject script payloads through the plugin settings page that execute in the browsers of all WordPress users viewing the site, enabling cookie theft and sensitive data exfiltration.	6.4	More Details
CVE-2026-6174	The CC Child Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'more' parameter in all versions up to, and including, 2.1.1 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-2026-6252	The Meta Field Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tagName' block attribute in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6646	The The7 theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'dt_default_button' shortcode in all versions up to, and including, 14.3.2. This is due to insufficient input sanitization and output escaping on the 'title' component of the 'link' shortcode parameter. 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-2020-37240	Queue Management System 4.0.0 contains a stored cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through user creation fields. Attackers can insert JavaScript payloads in the First Name, Last Name, and Email fields during user creation, which execute when viewing the User List page.	6.4	More Details
CVE-2026-3004	The Snow Monkey Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘data-slick' attribute in all versions up to, and including, 24.1.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6962	The Cost of Goods: Product Cost & Profit Calculator for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'alg_wc_cog_product_cost' and 'alg_wc_cog_product_profit' shortcodes in all versions up to, and including, 4.1.0 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-2021-47962	Savsoft Quiz 5.0 contains a persistent cross-site scripting vulnerability in the user account settings page that allows authenticated attackers to inject malicious HTML and JavaScript code. Attackers can inject script payloads into user profile fields at the edit_user endpoint, which execute in the browsers of users viewing the affected profile after submission.	6.4	More Details
CVE-2021-47968	Podcast Generator 3.1 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting unfiltered JavaScript code in the long_description parameter. Attackers can inject script tags through episode creation or editing requests to execute arbitrary JavaScript when other users view the episode details.	6.4	More Details
CVE-2026-8201	A use-after-free vulnerability exists in MongoDB's Field-Level Encryption (FLE) query analysis component, affecting client-side uses of mongocryptd and crypt_shared. Triggering this vulnerability requires control over the structure of a client's FLE-related query. This issue impacts MongoDB Server's mongocryptd component v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	6.4	More Details
CVE-2026-6828	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'permission_message' parameter in all versions up to, and including, 6.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5361	The Envira Gallery Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the REST API in versions up to and including 1.12.4. This is due to insufficient input sanitization in the update_gallery_data() function and improper output escaping in the gallery_init() function. The sanitize_config_values() function only sanitizes the justified_gallery_theme and justified_row_height parameters, but does not sanitize the arrows parameter. When the arrows value is output in the inline JavaScript configuration, it uses esc_attr() which is designed for HTML attribute contexts, not JavaScript contexts, allowing JavaScript expression injection. 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-2026-5243	The The Plus Addons for Elementor – Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to stored cross-site scripting via the `menu_hover_click` parameter of the Navigation Menu Lite widget in all versions up to, and including, 6.4.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6415	The Advanced Custom Fields: Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 5.0.2. This is due to insufficient input validation of JSON field values and unsafe client-side HTML construction in the update_preview() JavaScript 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-2026-2695	A command injection vulnerability was discovered in TeamViewer DEX Platform On-Premises (former 1E DEX Platform On-Premises) prior to version 9.2. Improper input validation allows authenticated users with at least questioner privileges to inject commands in specific instructions. Exploitation could lead to execution of elevated commands on devices connected to the platform.	6.3	More Details
CVE-2026-8733	A vulnerability was found in Investintech SlimPDFReader up to 2.0.13. Affected by this vulnerability is the function sub_3B4610 of the file SlimPDFReader.exe. The manipulation results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor responded to the initial vulnerability report by the researcher with a note that the product is discontinued. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-8735	A vulnerability was identified in Oinone Pamirs up to 7.2.0. This affects the function JsonUtils.parseMap of the file PamirsParserConfig.java of the component appConfigQuery Interface. Such manipulation leads to deserialization. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-44408	There is an unauthorized access vulnerability in ZTE MU5250. Due to improper permission control of the Web interface, an unauthorized attacker can modify configuration through the interface.	6.3	More Details
CVE-2026-8774	A vulnerability was detected in Edimax BR-6228NC 1.22. Affected by this issue is the function mp of the file /goform/mp of the component POST Request Handler. The manipulation of the argument command results in command injection. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-8786	A vulnerability has been found in Tencent WeKnora up to 0.3.6. Affected by this issue is the function getKnowledgeBaseForInitialization of the file internal/handler/initialization.go of the component Config API Endpoint. The manipulation of the argument kbId leads to authorization bypass. 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-2026-8753	A security vulnerability has been detected in kalcaddle Kodbox up to 1.64. This issue affects the function parseVideoInfo of the file /workspace/source-code/plugins/fileThumb/lib/VideoResize.class.php of the component fileThumb Plugin. The manipulation of the argument ffmpegBin leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-69443	Remote Code Execution in coleam00 Archon 0.1.0. A crafted HTML page, when accessed by a victim, can execute commands, run prompts on behalf of the user, control the Archon UI features, and steal all Archon information available on the UI including API keys.	6.3	More Details
CVE-2026-8777	A vulnerability was found in Edimax BR-6428NS 1.10. This issue affects the function formStaDrvSetup of the file /goform/formStaDrvSetup of the component POST Request Handler. Performing a manipulation of the argument stadrv_ssid results in command 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-2026-8743	A vulnerability was found in Open5GS up to 2.7.6. This impacts the function ran_ue_find_by_amf_ue_ngap_id of the file src/amf/context.c of the component AMF/MME. Performing a manipulation results in improper authorization. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The patch is named 5746b8576cfceec18ed87eb7d8cf11b1fb4cd8b1. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-	A flaw has been found in Sanluan PublicCMS 5.202506.d. The impacted element is the function execute of the file publiccms-core/src/main/java/com/publiccms/views/directive/tools/TemplateResultDirective.java of the component templateResult API. This manipulation of the argument templateContent causes improper neutralization of special elements used in a template engine. The	6.3	More

8740	attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2026-33380	A vulnerability in SQL Expressions allows an authenticated attacker to read arbitrary files from the Grafana server's filesystem. Only instances with the sqlExpressions feature toggle enabled are vulnerable.	6.3	More Details
CVE-2025-67031	ORSEE (Online Recruitment System for Economic Experiments) 3.1.0 contains an authenticated Remote Code Execution vulnerability in the participant profile field processing subsystem. Certain field configurations accept values beginning with the prefix "func:" which are passed directly into an eval() call inside tagsets/participant.php and tagsets/options.php.	6.3	More Details
CVE-2026-8754	A vulnerability was detected in AstrBotDevs AstrBot up to 4.23.5. Impacted is the function post_file of the file astrbot/dashboard/routes/chat.py of the component File Upload Handler. The manipulation of the argument filename results in path traversal. It is possible to launch the attack remotely. The exploit is now public and may be used. Upgrading to version 4.23.6 is recommended to address this issue. The patch is identified as aaec41e5054569ceaa1113593a34da7568e2d211. You should upgrade the affected component.	6.3	More Details
CVE-2026-8747	A weakness has been identified in Z-BlogPHP 1.7.4.3430. This affects the function CheckComment of the file zb_system/function/c_system_event.php of the component Commend Approval Handler. This manipulation causes improper authorization. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2024-51395	Buffer Overflow vulnerability in Ardupiot Copter Latest commit 92693e023793133e49a035daf37c14433e484778 allows a local attacker to cause a denial of service via the AP_SmartAudio::loop, AP_SmartAudio, AP_SmartAudio.cpp components.	6.2	More Details
CVE-2026-41969	Permission control vulnerability in the projection module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2020-37246	Supsystic Backup 2.3.9 contains a local file inclusion vulnerability that allows unauthenticated attackers to read and delete arbitrary files by manipulating the download path parameter. Attackers can modify the download parameter in admin.php requests with directory traversal sequences to access sensitive files like /etc/passwd or delete files via the removeAction parameter.	6.2	More Details
CVE-2024-48519	Buffer Overflow vulnerability in Ardupilot rover commit v.c56439b045162058df0ff136afea3081fcd06d38 allows a local attacker to cause a denial of service via the AP_InertialSensor_ADIS1647x.cpp, ArduRover, ADIS1647x Sensor component.	6.2	More Details
CVE-2020-37234	Internet Download Manager 6.38.12 contains a buffer overflow vulnerability in the Scheduler component that allows local attackers to crash the application by supplying oversized input. Attackers can paste malicious data exceeding 5000 bytes into the 'Open the following file when done' field to trigger a denial of service condition.	6.2	More Details
CVE-2026-38719	OpENer v2.3-558-g1e99582 contains an out-of-bounds read vulnerability in the Common Packet Format (CPF) parser, specifically in CreateCommonPacketFormatStructure() in source/src/enet_encap/cpf.c. A crafted ENIP/CPF message can supply an attacker-controlled item_count value that is not consistently validated against the remaining data_length of the CPF slice	6.2	More Details
CVE-2021-47978	ProcessMaker 3.5.4 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting improper path traversal validation. Attackers can send requests with directory traversal sequences to access sensitive system files like /etc/passwd without authentication.	6.2	More Details
CVE-2018-25324	Simple Fields 0.2 through 0.3.5 WordPress Plugin contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by injecting null bytes into the wp_abspath parameter on PHP versions before 5.3.4. Attackers can supply malicious wp_abspath values to simple_fields.php to include files like /etc/passwd or inject PHP code into Apache logs for remote code execution when allow_url_include is enabled.	6.2	More Details
CVE-2025-15345	The MapGeo – Interactive Geo Maps plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'map' parameter in the display-map shortcode in all versions up to, and including, 1.6.27 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-2026-45028	Astro is a web framework. Astro versions prior to 6.1.10 used AES-GCM encryption to protect the confidentiality and integrity of server island props and slots parameters, but did not bind the ciphertext to its intended component or parameter type. An attacker could replay one component's encrypted props (p) value as another component's slots (s) value, or vice versa. Since slots contain raw unescaped HTML while props may contain user-controlled values, this could lead to XSS in applications. This occurs when the application uses server islands, two different server island components share the same key name for a prop and a slot, and an attacker has full control over the value of the overlapping prop (requires a dynamically rendered page). This vulnerability is fixed in 6.1.10.	6.1	More Details
CVE-2026-45231	DumbAssets through 1.0.11 contains a stored cross-site scripting vulnerability in asset fields including name, description, modelNumber, serialNumber, and tags that are stored without server-side sanitization and rendered using innerHTML without client-side escaping. Attackers can create or update assets with HTML or JavaScript payloads via the asset API endpoints to execute arbitrary scripts in the browsers of users viewing the asset list, and with Content-Security-Policy disabled, the injected scripts can make unrestricted connections to internal network services.	6.1	More Details
CVE-2026-6417	The GLS Shipping for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'failed_orders' parameter in all versions up to, and including, 1.4.0 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-2026-8656	Versions of the package jsondiffpatch before 0.7.6 are vulnerable to Cross-site Scripting (XSS) via the annotated formatter due to improper sanitization of JSON values and property names. If an application compares untrusted JSON/object data and renders annotated formatter output in the DOM, attacker-controlled HTML can be interpreted by the browser, resulting in XSS.	6.1	More Details
CVE-2026-45243	Summarize prior to 0.15.1 contains a missing authorization vulnerability in the content script window.postMessage bridge that allows malicious pages to perform unauthorized operations on automation artifacts. Attackers can simulate runtime messages with spoofed sender identifiers to list, read, create, overwrite, or delete automation artifacts scoped to the affected tab without proper authorization checks.	6.1	More Details

CVE-2026-29965	HSC MailInspector 5.3.3-7 is vulnerable to Cross Site Scripting (XSS) in the /police/WarningUrlPage.php endpoint due to improper neutralization of user-supplied input that uses alternate or obfuscated JavaScript syntax.	6.1	More Details
CVE-2026-41932	Vvveb before 1.0.8.3 contains a stored cross-site scripting vulnerability in the customer signup flow where the Signup::addUser() controller copies raw POST username values into the display_name field before sanitization occurs. Attackers can submit HTML and script markup in the username field during signup, which gets stripped from the username column but persisted verbatim in the display_name column, allowing stored XSS execution when display_name is rendered without encoding in vulnerable views.	6.1	More Details
CVE-2026-29964	HSC MailInspector v5.3.3-7 contains a Cross-Site Scripting (XSS) vulnerability in the /tap/tap.php endpoint due to improper neutralization of user-controlled input using alternate or obfuscated JavaScript syntax. The endpoint reflects unsanitized user input in HTTP responses without adequate output encoding, allowing a remote attacker to execute arbitrary JavaScript code in the context of a victim's browser.	6.1	More Details
CVE-2026-24710	Northern.tech CFEngine Enterprise before 3.21.8, 3.24.3, and 3.27.0 allows XSS.	6.1	More Details
CVE-2026-44664	fast-xml-builder builds XML from JSON. In 1.1.5, the fix for CVE-2026-41650 in fast-xml-parser sanitizes -- sequences in XML comment content using .replace(/--/g, '- -'). This skip the values containing three consecutive dashes (e.g., --->...), allowing an attacker to break out of an XML comment and inject arbitrary XML/HTML content. This vulnerability is fixed in 1.1.6.	6.1	More Details
CVE-2021-47967	PHP Timeclock 1.04 contains multiple cross-site scripting vulnerabilities that allow unauthenticated attackers to inject arbitrary JavaScript by manipulating URL paths and POST parameters. Attackers can append malicious payloads to login.php, timeclock.php, audit.php, and timerpt.php endpoints, or inject code through from_date and to_date parameters in report requests to execute scripts in user browsers.	6.1	More Details
CVE-2026-45314	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, the channel webhook create/update flow accepts arbitrary profile_image_url values, including ... payloads. The profile image endpoint then decodes and serves this SVG as image/svg+xml without sanitization, allowing attacker-controlled script handlers (for example onload) to execute when the profile-image URL is opened in the browser. This vulnerability is fixed in 0.9.3.	6.1	More Details
CVE-2026-44665	fast-xml-builder builds XML from JSON. Prior to 1.1.7, when an input data has quotes in attribute values but process entities is not enabled, it breaks the attribute value into multiple attributes. This gives the room for an attacker to insert unwanted attributes to the XML/HTML. This vulnerability is fixed in 1.1.7.	6.1	More Details
CVE-2026-41255	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.10 and 2.11.5, Access to the views via tokens or unauthenticated requests marked the endpoint as not requiring CSRF protection. The marking was a member variable in flask-wtf.csrf.CSRFProtect(), which was stored as a module level variable in the flask_app middleware. This API was never intended for request level changes, it is primarily a decorator for static configuration. An unauthenticated request could hit a protected endpoint, exempting it from CSRF protection for the life of the particular server process. (e.g. one worker of uwsgi). This vulnerability is fixed in 2.10.10 and 2.11.5.	6.1	More Details
CVE-2026-31379	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.1	More Details
CVE-2026-42207	Magento Long Term Support (LTS) is an unofficial, community-driven project provides an alternative to the Magento Community Edition e-commerce platform with a high level of backward compatibility. Prior to 20.18.0, Mage_ProductAlert_AddController::stockAction() reads the uenc query parameter and passes it directly to $this->_redirectUrl($backUrl) without calling $this->_isUrlInternal(). When the supplied product_id does not match any catalog product, the server issues an unvalidated HTTP 302 redirect to whatever URL was provided as uenc. This vulnerability is fixed in 20.18.0.	6.1	More Details
CVE-2018-25331	Zenar Content Management System contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating form parameters in POST requests. Attackers can inject script tags through the current_page parameter sent to the ajax.php endpoint, which reflects unsanitized user input in the response HTML to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2026-44376	CubeCart is an ecommerce software solution. Prior to 6.7.0, an unauthenticated Reflected XSS vulnerability exists in the CubeCart v6.x search feature. Due to a logic flaw in classes/catalogue.class.php, user input is reflected without sanitization only when a search returns exactly one product. This flaw bypasses current filters, allowing an attacker to execute malicious JavaScript in the victim's browser, leading to session hijacking, site defacement, or phishing. This vulnerability is fixed in 6.7.0.	6.1	More Details
CVE-2026-44580	Next.js is a React framework for building full-stack web applications. From 13.0.0 to before 15.5.16 and 16.2.5, applications that use beforeInteractive scripts together with untrusted content can be vulnerable to cross-site scripting. In affected versions, serialized script content was not escaped safely before being embedded into the document, which could allow attacker-controlled input to break out of the intended script context and execute arbitrary JavaScript in a visitor's browser. This vulnerability is fixed in 15.5.16 and 16.2.5.	6.1	More Details
CVE-2026-8496	A cross-site scripting (XSS) vulnerability exists in Alinto SOGo, version 5.12.7. A maliciously crafted ICS calendar invitation files allows arbitrary JavaScript execution within the authenticated SOGo webmail session. The issue occurs because SVG content embedded in the description field of an ICS file, with an onrepeat event handler, is insufficiently sanitized before being rendered in the webmail interface. A remote attacker can execute JavaScript in the victim's browser when the malicious calendar invite is viewed. Successful exploitation may allow mailbox access, email and contact theft, session hijacking, and other actions allowed by an authenticated user.	6.1	More Details
CVE-2026-31906	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	6.1	More Details
CVE-2026-44366	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.1, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Vvveb CMS comment submission flow. The author field is submitted by an unauthenticated user on any public post page, stored without sanitization, and later rendered unsanitized in two distinct sinks: This vulnerability is fixed in 1.0.8.1.	6.1	More Details
CVE-2025-40902	A Stored HTML Injection vulnerability was discovered in the Users functionality due to improper validation of an input parameter. An authenticated user with administrative privileges can create a malicious user whose username contains HTML tags. When a victim attempts to delete a group containing the affected user, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	5.9	More Details

CVE-2026-42597	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, the /forms/chromium/convert/url and /forms/chromium/screenshot/url routes accept url=file:///tmp/... from anonymous callers. The default Chromium deny-list intentionally exempts file:///tmp/ so HTML/Markdown routes can load their own request-local assets, and those routes apply a per-request AllowedFilePrefixes guard to scope the read. The URL routes never set AllowedFilePrefixes, so the scope guard silently skips. Alice enumerates /tmp/, walks Gotenberg's per-request working directories, and reads the raw source files of other in-flight conversions as rendered PDF output. This vulnerability is fixed in 8.32.0.	5.9	More Details
CVE-2026-6811	Stack exhaustion vulnerability in the MongoDB PHP driver can cause application crashes when processing deeply nested BSON documents in unusual circumstances when the source of these BSON documents is not MongoDB Server.	5.9	More Details
CVE-2025-40903	A Stored HTML Injection vulnerability was discovered in the Schedule Restore Archive functionality due to improper validation of an input parameter. An authenticated user with administrative privileges can define a malicious restore schedule containing HTML tags. When a victim views the affected schedule, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	5.9	More Details
CVE-2026-41967	Permission control vulnerability in the manufacturability design module. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2026-41968	Permission control vulnerability in the manufacturability design module. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2026-44448	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.102.0 and 16.11.0, certain endpoints failed to enforce proper authorization checks, allowing users to modify data beyond their permitted role. This vulnerability is fixed in 15.102.0 and 16.11.0.	5.9	More Details
CVE-2026-41961	Permission control vulnerability in contacts. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2025-40901	A Stored HTML Injection vulnerability was discovered in the Credentials Manager functionality due to improper validation of an input parameter. An authenticated user with administrative privileges can define a malicious identity containing HTML tags. When a victim attempts to delete the affected identity, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	5.9	More Details
CVE-2026-6253	curl might erroneously pass on credentials for a first proxy to a second proxy. This can happen when the following conditions are true: 1. curl is setup to use specific different proxies for different URL schemes 2. the first proxy needs credentials 3. the second proxy uses no credentials 4. while using the first proxy (using say `http://`), curl is asked to follow a redirect to a URL using another scheme (say `https://`), accessed using a second, different, proxy	5.9	More Details
CVE-2026-32134	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. In versions 0.24.10 and below, when NanoMQ handles high-concurrency reconnect traffic using a reconnect-collision payload, the broker can crash due to a NULL pointer dereference during MQTT session resumption for clean_start=0 clients. The transport's p_peer callback (tcptran_pipe_peer()) iterates cpipe->subinfol while copying session metadata from the cached old pipe to the new reconnecting pipe, without checking whether the pointer is NULL. Under a reconnect race, cpipe->subinfol can be freed and set to NULL before session restore invokes this function, resulting in a remote unauthenticated Denial-of-Service (process crash) condition. This issue has been fixed in version 0.24.11.	5.9	More Details
CVE-2026-41470	LIVE555 before 2026.04.22 contains an authorization bypass vulnerability in RTSP session command handling that allows attackers to replay valid Session tokens from unauthenticated connections. Attackers who obtain a valid Session token can issue PLAY and TEARDOWN commands from a second TCP connection without authentication, causing server crashes through virtual function call errors or disrupting active streams by terminating victim sessions.	5.9	More Details
CVE-2026-44577	Next.js is a React framework for building full-stack web applications. From 10.0.0 to before 15.5.16 and 16.2.5, when self-hosting Next.js with the default image loader, the Image Optimization API fetches local images entirely into memory without enforcing a maximum size limit. An attacker could cause out-of-memory conditions by requesting large local assets from the /_next/image endpoint that match the images.localPatterns configuration (by default, all patterns are allowed). This vulnerability is fixed in 15.5.16 and 16.2.5.	5.9	More Details
CVE-2026-33381	When a user's access to mint tokens for a service account is revoked, it is sometimes still possible to do so for a few seconds after the event. The user will eventually lose access to do this.	5.9	More Details
CVE-2026-41949	Dify version 1.14.1 and prior contain an authorization bypass vulnerability in the file preview endpoint that allows any authenticated user to read up to 3,000 characters of any uploaded document across all tenants and workspaces using only the file's UUID. Attackers can access the /console/api/files/{file_id}/preview endpoint with an intercepted file UUID to extract sensitive content from documents without ownership or workspace permission verification. NOTE: Dify Cloud allows unauthenticated free self-registration, making account creation trivially accessible to any attacker.	5.9	More Details
CVE-2026-4873	A vulnerability exists where a connection requiring TLS incorrectly reuses an existing unencrypted connection from the same connection pool. If an initial transfer is made in clear-text (via IMAP, SMTP, or POP3), a subsequent request to that same host bypasses the TLS requirement and instead transmit data unencrypted.	5.9	More Details
CVE-2026-42581	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, HttpObjectDecoder strips a conflicting Content-Length header when a request carries both Transfer-Encoding: chunked and Content-Length, but only for HTTP/1.1 messages. The guard is absent for HTTP/1.0. An attacker that sends an HTTP/1.0 request with both headers causes Netty to decode the body as chunked while leaving Content-Length intact in the forwarded HttpMessage. Any downstream proxy or handler that trusts Content-Length over Transfer-Encoding will disagree on message boundaries, enabling request smuggling. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	5.8	More Details
CVE-2026-41960	Permission control vulnerability in calls. Impact: Successful exploitation of this vulnerability may affect availability.	5.8	More Details

CVE-2026-41181	Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.44, 3.6.15, and 3.7.0-rc.3, there is an information disclosure vulnerability in Traefik's errors (custom error pages) middleware. When the backend returns a response matching the configured status range, the middleware forwards the original request's complete header set, including Authorization, Cookie, and other authentication material, to the separate error page service rather than only the minimal context needed to render the error page. This behavior is undocumented: the documentation states only that Host is forwarded by default, so operators are not warned that sensitive credentials are shared across service boundaries. Deployments using the errors middleware with a distinct error page service may inadvertently expose end-user credentials to infrastructure that was not intended to receive them. This vulnerability is fixed in 2.11.44, 3.6.15, and 3.7.0-rc.3.	5.8	More Details
CVE-2026-44312	css_parser is a Ruby CSS parser. Prior to 2.1.0 and 1.22.0, the CSS Parser gem does not validate HTTPS connections, allowing a Man-in-the-Middle (MITM) attacker to inject or modify CSS content when stylesheets are loaded via HTTPS. The connection is established with OpenSSL::SSL::VERIFY_NONE, meaning any HTTPS certificate—even entirely untrusted—will be accepted without validation. This vulnerability is fixed in 2.1.0 and 1.22.0.	5.8	More Details
CVE-2026-45557	Technitium DNS Server aggressively tries to fetch missing RRSIG records or mismatched DNSKEY records. An attacker in control of a domain can cause a vulnerable system to generate excessive network traffic. Fixed in 15.0.	5.8	More Details
CVE-2026-44002	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, vm2's CallSite wrapper class (intended as a safe wrapper for V8's native CallSite) blocks getThis() and getFunction() to prevent host object leakage, but allows getFileName() to return unsanitized host absolute paths. Any sandboxed code can extract the full directory structure, library paths, and framework versions of the host server. This vulnerability is fixed in 3.11.0.	5.8	More Details
CVE-2026-3160	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.7 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to view Jira issues outside the configured project scope due to an integration filter functioning only as a display control rather than enforcing access boundaries as specified.	5.8	More Details
CVE-2026-42926	When NGINX Open Source is configured to proxy HTTP/2 traffic by setting proxy_http_version to 2, and also uses proxy_set_body, an attacker may be able to inject frame headers and payload bytes to the upstream peer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.8	More Details
CVE-2026-34600	Joplin is an open source note-taking and to-do application that organises notes and lists into notebooks. Versions 3.5.2 and prior contain a logic error in the delta API that allows share recipients to download notes that are no longer shared with them, related to but not fully fixed by the prior patch in #14289. In ChangeModel.delta, when DELTA_INCLUDES_ITEMS is enabled (the default), the latest state of items is attached to delta output without verifying that those items are still shared with the requesting user, and the existing removal logic only filters items deleted for all users. Additionally, the change compression logic incorrectly reduces create - delete to NOOP, which is unsafe because compression is applied per page and an item can have multiple create events; if an earlier create falls on a separate page from a later create -> delete pair, the deletion is dropped and the sequence collapses to a create. As a result, the delta API returns a create event for a deleted item with the full latest content attached, exposing notes the user no longer has access to. This issue has been fixed in version 3.5.3.	5.7	More Details
CVE-2026-44520	Docling-Graph turns documents into validated Pydantic objects, then builds a directed knowledge graph with explicit semantic relationships. Prior to 1.5.1, the URLInputHandler class in docling_graph/core/input/handlers.py makes HTTP requests to user-supplied URLs without validating whether the target resolves to a private, loopback, or link-local IP address. The URLValidator only checks for a valid scheme and non-empty netloc, performing no IP-level validation. Additionally, requests.head() was called with allow_redirects=True, allowing an attacker to redirect requests to internal endpoints via an intermediary URL. An attacker who can control the --source CLI argument or PipelineConfig.source API parameter can trigger Server-Side Request Forgery (SSRF). This vulnerability is fixed in 1.5.1.	5.7	More Details
CVE-2025-29338	NXP moal.ko Wi-Fi driver 5.1.7.10 FW version from v17.92.1.p149.43 To v17.92.1.p149.157 was discovered to contain a buffer overflow via the mod_para parameter in the woal_init_module_param function.	5.6	More Details
CVE-2026-41965	Use-After-Free (UAF) vulnerability in the web. Impact: Successful exploitation of this vulnerability may affect availability.	5.6	More Details
CVE-2026-41966	Permission control vulnerability in the smart sensing service. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.6	More Details
CVE-2026-44479	Vercel’s AI Cloud is a unified platform for building modern applications. From 50.16.0 to 52.0.0, hen the Vercel CLI runs in non-interactive mode (--non-interactive or auto-detected AI agent), commands that cannot complete autonomously emit JSON payloads with suggested follow-up commands. If the user authenticated via --token or -t on the command line, the token value is included verbatim in those suggestions. The plaintext token may be captured in CI/CD logs, agent transcripts, or other automation output. This vulnerability is fixed in 52.0.1.	5.5	More Details
CVE-2020-37169	WordPress Plugin ultimate-member 2.1.3 contains a local file inclusion vulnerability that allows authenticated attackers to include arbitrary files by manipulating the pack parameter in class-admin-upgrade.php. Attackers can send POST requests with malicious pack values to include unintended PHP files from the packages directory and execute arbitrary code.	5.5	More Details
CVE-2026-47309	Uncontrolled Recursion vulnerability in Samsung Open Source Escargot allows Oversized Serialized Data Payloads. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details
CVE-2026-47308	NULL pointer dereference vulnerability in Samsung Open Source Walrus allows Pointer Manipulation. This issue affects Walrus: f339b8ee4ea701772e8ae640b3d1b12ac02b1ae9.	5.5	More Details
CVE-2026-46333	In the Linux kernel, the following vulnerability has been resolved: ptrace: slightly saner 'get_dumpable()' logic The 'dumpability' of a task is fundamentally about the memory image of the task - the concept comes from whether it can core dump or not - and makes no sense when you don't have an associated mm. And almost all users do in fact use it only for the case where the task has a mm pointer. But we have one odd special case: ptrace_may_access() uses 'dumpable' to check various other things entirely independently of the MM (typically explicitly using flags like PTRACE_MODE_READ_FSCREDS). Including for threads that no longer have a VM (and maybe never did, like most kernel threads). It's not what this flag was designed for, but it is what it is. The ptrace code does check that the uid/gid matches, so you do have to be uid-0 to see kernel thread details, but this means that the traditional "drop capabilities" model doesn't	5.5	More Details

	make any difference for this all. Make it all make a *bit* more sense by saying that if you don't have a MM pointer, we'll use a cached "last dumpability" flag if the thread ever had a MM (it will be zero for kernel threads since it is never set), and require a proper CAP_SYS_PTRACE capability to override.		
CVE-2026-47307	NULL pointer dereference vulnerability in Samsung Open Source Walrus allows an attacker to cause a denial of service via a crafted WebAssembly module containing deeply nested instructions. This issue affects Walrus: f339b8ee4ea701772e8ae640b3d1b12ac02b1ae9.	5.5	More Details
CVE-2026-43996	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation. Prior to 3.0.18.0 and 3.1.13.0, the bounds check in TGAInput::decode_pixel computes k + palbytespp as unsigned 32-bit arithmetic. When k = 0xFFFFFFFC and palbytespp = 4, the addition wraps to 0, which compares less than palette_alloc_size and passes the check. The subsequent palette access uses the unwrapped k (0xFFFFFFFC) as the index, reading ~4 GB past the start of the palette buffer — SEGV. This vulnerability is fixed in 3.0.18.0 and 3.1.13.0.	5.5	More Details
CVE-2026-45246	Summarize prior to 0.15.1 contains an insecure file permission vulnerability in the refresh-free configuration rewrite path that allows local users to read sensitive credentials by exploiting default filesystem permissions. When the refresh-free path rewrites the configuration file, it creates the replacement with default process umask permissions instead of preserving the original file permissions, exposing the config file containing API keys and provider credentials to other local users on shared Unix-like systems.	5.5	More Details
CVE-2026-46383	Microsoft APM is an open-source, community-driven dependency manager for AI agents. Prior to 0.13.0, Microsoft APM contains a Windows-specific archive extraction boundary failure in the legacy-bundle probe used by apm install <bundle> on supported Python 3.10 and 3.11 runtimes. When apm install is given a local .tar.gz that is not recognized as a plugin-format bundle, APM probes whether it is a legacy --format apm bundle. On Python versions earlier than 3.12, that probe extracts untrusted tar members with raw tar.extractall() without rejecting Windows absolute member names such as D:/.... This vulnerability is fixed in 0.13.0.	5.5	More Details
CVE-2026-27766	in OpenHarmony v6.0 and prior versions allow a local attacker cause information leak.	5.5	More Details
CVE-2026-25850	in OpenHarmony v6.0 and prior versions allow a local attacker cause information leak	5.5	More Details
CVE-2026-41971	Permission control vulnerability in the security control module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2020-37174	WOOF Products Filter for WooCommerce 1.2.3 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by entering XSS payloads in design tab textfields. Attackers can inject JavaScript code through fields like 'Text for block toggle' and 'Custom front css styles' that executes on frontend pages when saved, affecting all site visitors.	5.5	More Details
CVE-2024-51394	Buffer Overflow vulnerability in Ardupiot Copter Latest commit 92693e023793133e49a035daf37c14433e484778 allows a local attacker to cause a denial of service via the AP_MSP::loop, AP_MSP, AP_MSP.cpp components.	5.5	More Details
CVE-2026-47317	Uncontrolled Recursion vulnerability in Samsung Open Source Escargot allows Excessive Allocation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details
CVE-2026-47315	Improper Check for Unusual or Exceptional Conditions vulnerability in Samsung Open Source Escargot allows Input Data Manipulation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details
CVE-2026-32849	NetBSD prior to commit ec8451e contains a signed integer overflow vulnerability in the cryptodev_op() function in sys/opencrypto/cryptodev.c where the local variable iov_len is declared as a signed int but assigned from an unsigned cop->dst_len value, causing undefined behavior when cop->dst_len exceeds INT_MAX. A local attacker with access to /dev/crypto and a compression session type can exploit this vulnerability by providing a dst_len value exceeding INT_MAX to trigger a kernel panic through NULL pointer dereference when CONFIG_SVS is disabled and corrupted UIO pointer arithmetic.	5.5	More Details
CVE-2026-21016	Incorrect privilege assignment in LocationManager prior to SMR May-2026 Release 1 allows local attackers to access sensitive information.	5.5	More Details
CVE-2025-14767	The WPC Badge Management for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' attribute of the `wpcbm_best_seller` shortcode in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2026-8586	Inappropriate implementation in Chromoting in Google Chrome prior to 148.0.7778.168 allowed a local attacker to bypass discretionary access control via a malicious file. (Chromium security severity: Medium)	5.5	More Details
CVE-2026-47316	Improper Check or Handling of Exceptional Conditions vulnerability in Samsung Open Source Escargot allows Input Data Manipulation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details
CVE-2026-21015	Incorrect default permissions in FactoryCamera prior to SMR May-2026 Release 1 allows local attacker to access unique identifier.	5.5	More Details
CVE-2026-21022	Improper handling of insufficient permissions in Routines prior to SMR May-2026 Release 1 allows local attackers to access sensitive information.	5.5	More Details
CVE-2026-47313	Memory allocation with excessive size value vulnerability in Samsung Open Source Escargot allows Excessive Allocation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details

CVE-2026-47312	Release of invalid pointer or reference vulnerability in Samsung Open Source Escargot allows Buffer Manipulation. This issue affects Escargot: 590345cc6258317c5da850d846ce6baaf2afc2d3.	5.5	More Details
CVE-2025-57798	Joplin is an open source note-taking and to-do application that organises notes and lists into notebooks. Versions 3.6.14 and prior contain a Denial of Service (DoS) vulnerability in the title input functionality due to a lack of proper length validation. This flaw allows an attacker to cause an Out Of Memory (OOM) error and subsequent program termination by inserting an excessively long string into a note's title. This can be triggered either through direct user interface (UI) input or programmatically via the local web service API after compromising an authentication token. There are 2 primary methods of exploitation: via User Interface (UI) Input, and the Local Web Service API. A local user can directly type or paste an extremely long string into the title field when creating or editing a note Joplin runs a local web service (typically on port 41184) that allows programmatic interaction, such as creating or editing notes via HTTP API calls. If an attacker manages to exfiltrate or compromise the user's authentication token (e.g., through malware on the local system, or other local vulnerabilities), they can then send a crafted HTTP POST request to this local API. By including an excessively long string in the title parameter of this request, the application will attempt to allocate an unbounded amount of memory. This issue has been patched in version 3.7.1.	5.5	More Details
CVE-2026-44564	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the ydoc:document:update Socket.IO event handler checks whether the sender is a member of the document's Socket.IO room (line 678) but does not verify that the sender has write permission. Users with read-only access join the document room via ydoc:document:join, which only requires read permission (line 520). Once in the room, the user can emit ydoc:document:update events that modify the in-memory Yjs document state and are broadcast to all other collaborators in real time. This vulnerability is fixed in 0.9.0.	5.4	More Details
CVE-2026-46360	phpMyFAQ before 4.1.2 contains a stored cross-site scripting vulnerability in SvgSanitizer::decodeAllEntities() that limits recursive entity decoding to 5 iterations, allowing attackers to bypass sanitization. Authenticated users with FAQ_EDIT permission can upload malicious SVG files with deeply nested ampersand encoding around numeric HTML entities to reconstruct javascript: URLs, which execute arbitrary JavaScript when clicked by other users viewing the uploaded SVG.	5.4	More Details
CVE-2026-1631	The Feeds for YouTube (YouTube video, channel, and gallery plugin) WordPress plugin before 2.6.4 is vulnerable to unauthorized modification of the Feeds for YouTube (YouTube video, channel, and gallery plugin) WordPress plugin before 2.6.4's license key due to a missing capability check on the 'actions' function. This makes it possible for subscribers and above delete the license key.	5.4	More Details
CVE-2026-45494	Microsoft Edge (Chromium-based) Spoofing Vulnerability	5.4	More Details
CVE-2026-45492	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	5.4	More Details
CVE-2021-47981	Quick.CMS 6.7 contains a cross-site scripting vulnerability in the sliders form that allows authenticated attackers to inject malicious scripts by submitting XSS payloads through the sDescription parameter. Attackers can craft CSRF forms targeting the admin.php?p=sliders-form endpoint to execute arbitrary JavaScript in victim browsers when the form is submitted.	5.4	More Details
CVE-2025-62310	HCL AION is affected by a vulnerability where encryption is not enforced for certain data transmissions or operations. This may expose sensitive information to potential interception or unauthorized access under specific conditions.	5.4	More Details
CVE-2026-23695	Cockpit CMS through version 2.14.0, patched in commit 72a83fc, contains a stored cross-site scripting vulnerability in the Set field type's Display template option, where the template string is processed by the $interpolate function using new Function() and rendered via Vue's v-html directive without sanitization. An attacker with content/:models/manage permission can inject arbitrary JavaScript into the Display template, which executes in the browser of any user viewing the collection items list.	5.4	More Details
CVE-2026-46365	phpMyFAQ before 4.1.2 contains a missing authorization vulnerability in the DELETE /admin/api/content/tags/{tagId} endpoint that allows any authenticated user to delete tags. Any logged-in user, including regular frontend users, can delete arbitrary tags by sending a DELETE request with a valid session cookie, resulting in permanent data loss and disruption of FAQ organization.	5.4	More Details
CVE-2026-44310	Gitsign is a keyless Sigstore to signing tool for Git commits with your a GitHub / OIDC identity. From 0.4.0 to before 0.15.0, CertVerifier.Verify() in pkg/git/verifier.go unconditionally dereferences certs[0] after sd.GetCertificates() without checking the slice length. A CMS/PKCS7 signed message with an empty certificate set is a structurally valid DER payload; GetCertificates() returns an empty slice with no error, causing an immediate index-out-of-range panic. On the gitsign --verify code path (the GPG-compatible mode invoked by git verify-commit), the panic is silently recovered by internal/io/streams.go's Wrap() function, which returns nil instead of an error. main.go then exits with code 0, causing exit-code-only verification callers to interpret the failed verification as success. This vulnerability is fixed in 0.15.0.	5.4	More Details
CVE-2026-44429	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.7, the public catalogue UI served at GET / (file internal/api/handlers/v0/ui_index.html) is vulnerable to stored cross-site scripting via the server.websiteUrl field of any published server.json. Server-side validation in internal/validators/validators.go (validateWebsiteURL) only checks that the URL parses, is absolute, and uses the https scheme; it does not reject quote characters. Client-side, the value is interpolated into a double-quoted href attribute via innerHTML, using a homegrown escapeHtml helper that performs the standard textContent → innerHTML round-trip. Per the HTML serialisation algorithm, that round-trip encodes only &, <, > and U+00A0 inside text nodes — it does not encode " or '. A literal " in websiteUrl therefore breaks out of the href attribute, allowing arbitrary on* event handlers to be appended to the same <a> element. The Content-Security-Policy on / is script-src 'self' 'unsafe-inline' https://cdn.tailwindcss.com, so the injected event handlers execute. Any user able to obtain a publish token (e.g. via POST /v0/auth/github-at with their own GitHub account, or POST /v0/auth/none on a deployment that has anonymous auth enabled) can plant a poisoned record visible to every visitor of the registry homepage. This vulnerability is fixed in 1.7.7.	5.4	More Details
CVE-2026-6335	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.11 before 18.11.3 that under certain conditions could have allowed an authenticated user to execute arbitrary code in another user's browser session due to improper sanitization.	5.4	More Details
CVE-2026-45228	Quark Drive before 0.8.5 contains a stored cross-site scripting vulnerability in the System Configuration page where the template renders push_config key names using Vue.js's v-html directive without escaping. Authenticated attackers can inject HTML or JavaScript payloads as key names through the POST /update endpoint, which are persisted to disk and executed in the browsers of all authenticated users accessing the System Configuration tab, allowing session cookie exfiltration and arbitrary authenticated actions.	5.4	More Details
CVE-			

2026-8561	Incorrect security UI in Fullscreen in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-46363	phpMyFAQ before 4.1.2 contains a stored cross-site scripting vulnerability in FAQ creation and update endpoints that bypass sanitization through encode-decode cycles. The vulnerability allows authenticated attackers with FAQ_ADD permission to inject malicious script tags via question or answer parameters, which execute in every visitor's browser when FAQ content is rendered with the raw Twig filter.	5.4	More Details
CVE-2026-45299	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, the profile_image_url field on the user profile update form accepted arbitrary data: URI values without MIME-type validation, resulting in a XSS vulnerability. This vulnerability is fixed in 0.8.0.	5.4	More Details
CVE-2026-6472	Missing authorization in PostgreSQL CREATE TYPE allows an object creator to hijack other queries that use search_path to find user-defined types, including extension-defined types. That is to say, the victim will execute arbitrary SQL functions of the attacker's choice. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	5.4	More Details
CVE-2026-43644	podinfo through 6.11.2 contains a reflected cross-site scripting vulnerability in the /echo and /api/echo endpoints where the echoHandler writes request body content directly to the response without setting explicit Content-Type or X-Content-Type-Options headers. Attackers can craft cross-origin HTML pages with auto-submitting forms containing script payloads in the request body, which are served as text/html due to Go's content type detection, allowing the reflected script to execute in the podinfo origin context when victims visit the attacker's page.	5.4	More Details
CVE-2026-8539	Script injection in SanitizerAPI in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	5.4	More Details
CVE-2026-45318	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, his advisory tracks a regression of the original Excel-preview XSS (CVE-2026-44549). The same root cause — XLSX.utils.sheet_to_html() output rendered via {@html excelHtml} without DOMPurify — was reintroduced sometime after v0.8.0 and is exploitable again This vulnerability is fixed in 0.9.3.	5.4	More Details
CVE-2025-12669	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.11 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to inject HTML and JavaScript into email notifications sent to other users due to improper input sanitization.	5.4	More Details
CVE-2026-22707	Strapi is an open source headless content management system. In Strapi versions prior to 5.33.3, the Upload plugin's Content API endpoints did not enforce the administrator-configured MIME type restrictions (`plugin.upload.security.allowedTypes` and `deniedTypes`). The same restrictions were correctly enforced on the Admin Panel upload path. The upload plugin's `enforceUploadSecurity` security check was invoked in the admin upload controller but was missing from the Content API controller. The Content API handlers `uploadFiles` and `replaceFile` (and the `upload` wrapper that dispatches to them) called the underlying upload service directly, bypassing both the magic-byte MIME detection and the configured allow/deny lists. An authenticated user with the Content API upload permission could therefore upload file types the administrator had explicitly disallowed, including HTML and SVG content. In deployments serving uploaded files from the same origin as the admin panel (default), an attacker could upload an HTML or SVG file that, when opened directly by an admin, executed JavaScript in the admin origin, enabling admin-session hijack and authenticated administrative actions against the admin API. The patch in version 5.33.3 introduces a shared `prepareUploadRequest` helper that wraps `enforceUploadSecurity` and is called from both the Content API and admin upload controllers, ensuring identical security policy enforcement on every upload entry point.	5.4	More Details
CVE-2018-25334	Zechat 1.5 contains a Cross-Site Request Forgery (CSRF) vulnerability that allows an attacker to change a user's information by bypassing anti-CSRF protections. The application uses a CSRF token, but an attacker can use the hashtag parameter to inject an encoded payload and bypass the CSRF protection, allowing for unauthorized changes to user data. This can be exploited by tricking a user into submitting a crafted form or by using a script to obtain and set the CSRF token.	5.4	More Details
CVE-2025-62313	HCL AION is affected by a vulnerability where adequate protections against brute-force attempts are not enforced. This may allow repeated authentication attempts, potentially leading to unauthorized access or account compromise under certain conditions.	5.4	More Details
CVE-2026-40703	A cross-site request forgery (CSRF) vulnerability exists in the dashboard of the BIG-IP Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.4	More Details
CVE-2026-45365	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.11, an internal-only bypass_filter parameter is exposed on the /openai/chat/completions and /ollama/api/chat HTTP endpoints via FastAPI query string binding, allowing any authenticated user to append ?bypass_filter=true and bypass model access control checks to invoke admin-restricted models. This vulnerability is fixed in 0.8.11.	5.4	More Details
CVE-2026-44561	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the is_user_channel_member function checks whether a ChannelMember row exists but does not check the is_active field. When a user is deactivated from a group or DM channel (removed by the channel owner, or leaves voluntarily), their membership row persists with is_active=False and status='left'. Because the authorization check ignores this field, the deactivated user retains full read and write access to the channel via direct API calls. This vulnerability is fixed in 0.9.0.	5.4	More Details
CVE-2026-20209	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker with read-only permissions to elevate their privileges from low to high and perform actions as a high-privileged user. This vulnerability exists because sensitive session information is recorded in audit logs. An attacker could exploit this vulnerability by elevating their read-only permissions in Cisco Catalyst SD-WAN Manager to those of a high-privileged user. A successful exploit could allow the attacker to perform actions as a high-privileged user.	5.4	More Details
CVE-2026-20210	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker with read-only permissions to modify configurations and perform unauthorized actions on an affected system. This vulnerability exists because of a failure to redact sensitive information within device configurations and templates. An attacker could exploit this vulnerability by elevating their read-only permissions to those of a high-privileged user. A successful exploit could allow the attacker to access or modify configuration settings within Cisco Catalyst SD-WAN Manager as a high-privileged user.	5.4	More Details
CVE-2026-	A flaw was found in Keycloak. When both realm-level and client-level `notBefore` revocation policies are configured, Keycloak's OpenID Connect (OIDC) Introspection feature fails to properly honor the realm-level policy. This allows tokens that should have been revoked to remain active, potentially leading to unauthorized access or continued session validity. This could impact the security of systems	5.4	More Details

8922	utilizing Keycloak for identity and access management.		
CVE-2026-45244	Summarize prior to 0.15.1 contains a missing authorization vulnerability that allows attackers to execute browser automation actions without per-call user approval when the extension automation feature is enabled. Attackers can influence the agent through malicious page or summary content to invoke enabled extension automation tools such as navigation or debugger-backed actions, bypassing the final user approval step when a user interacts with attacker-controlled content.	5.4	More Details
CVE-2026-44558	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the channel router does not call filter_allowed_access_grants on either create or update paths. A non-admin user who can create group channels (or who owns a channel) can submit arbitrary access grants — including public wildcard grants — and those grants are stored verbatim, bypassing the admin's permission framework. This vulnerability is fixed in 0.9.0.	5.4	More Details
CVE-2026-45396	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, the POST /api/v1/evaluations/feedback endpoint in Open WebUI v0.9.2 is vulnerable to mass assignment via FeedbackForm, which uses model_config = ConfigDict(extra='allow'). Due to an insecure dictionary merge order in insert_new_feedback(), an authenticated attacker can inject a user_id field in the request body that overwrites the server-derived value, creating feedback records attributed to any arbitrary user. This corrupts the model evaluation leaderboard (Elo ratings) and enables identity spoofing. This vulnerability is fixed in 0.9.5.	5.4	More Details
CVE-2026-7051	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 8.9.0. This is due to a missing ownership verification in the B2S_Post_Tools::deleteUserPublishPost() and B2S_Post_Tools::deleteUserSchedPost() functions, neither function includes a blog_user_id constraint in its database query, allowing authenticated attackers to soft-delete any user's B2S post records by supplying arbitrary sequential wp_b2s_posts.id values via the 'postId' parameter. This makes it possible for authenticated attackers to delete other users' published and scheduled social media post records, disrupting content publishing workflows.	5.4	More Details
CVE-2026-44563	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the /api/generate, /api/embed, /api/embeddings, and /api/show endpoints accept any model name from the user and forward the request to the Ollama backend without checking whether the user is authorized to access that model. These endpoints only require get_verified_user (any authenticated non-pending user) and validate that the model exists in the full unfiltered model list, but never check AccessGrants.has_access(). This vulnerability is fixed in 0.9.0.	5.4	More Details
CVE-2026-45346	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.31, there is a Cross-Site Scripting vulnerability in Open WebUI SVG renderer implementation. This vulnerability is fixed in 0.6.31.	5.4	More Details
CVE-2026-3829	The WP Encryption – One Click Free SSL Certificate & SSL / HTTPS Redirect, Security & SSL Scan plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the 'wple_basic_get_requests' function in all versions up to, and including, 7.8.5.10. This makes it possible for authenticated attackers, with subscriber level access and above, to reset the SSL setup state, force SSL to appear complete, and modify plan selection options.	5.4	More Details
CVE-2021-47955	CouchCMS 2.2.1 contains a cross-site scripting vulnerability that allows authenticated attackers to execute arbitrary JavaScript by uploading malicious SVG files through the file upload functionality. Attackers can upload SVG files containing embedded script tags to the browse.php endpoint, which are then executed in users' browsers when the files are accessed or previewed.	5.4	More Details
CVE-2026-36827	A command injection vulnerability exists in Panabit PAP-XM320 up to and including V7.7. The web management interface invokes the backend helper /usr/sbin/pappiw and passes user-controlled parameters to it. The helper performs unsafe argument processing using eval, which allows command injection when attacker-controlled input is included in the arguments. As a result, an authenticated remote attacker with access to the management interface may execute arbitrary shell commands.	5.4	More Details
CVE-2026-44425	ShellHub is a centralized SSH gateway. Prior to 0.24.2, the device list endpoint accepts user-controlled identifiers in the the name field of each filter property in the base64-encoded filter query parameter and the sort_by query parameter, which are then passed directly as BSON/SQL keys in the database layer without validation. Any authenticated user can craft payloads that cause the aggregation / query to fail and the API to return HTTP 500 with no body, with no rate limiting applied. This vulnerability is fixed in 0.24.2.	5.4	More Details
CVE-2026-44576	Next.js is a React framework for building full-stack web applications. From 14.2.0 to before 15.5.16 and 16.2.5, applications using React Server Components can be vulnerable to cache poisoning when shared caches do not correctly partition response variants. Under affected conditions, an attacker can cause an RSC response to be served from the original URL and poison shared cache entries so later visitors receive component payloads instead of the expected HTML. This vulnerability is fixed in 15.5.16 and 16.2.5.	5.4	More Details
CVE-2026-44003	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, vm2's code transformer has a performance optimization that skips AST analysis when the code does not contain catch, import, or async keywords. This fast-path bypass allows sandboxed code to directly access the internal VM2_INTERNAL_STATE_DO_NOT_USE_OR_PROGRAM_WILL_FAIL variable, which exposes internal security functions (handleException, wrapWith, import). This vulnerability is fixed in 3.11.0.	5.3	More Details
CVE-2026-45397	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, GET /api/v1/retrieval/ returns live RAG pipeline configuration to any unauthenticated HTTP client. No Authorization header, cookie, or API key is required. Every adjacent endpoint on the same router (/embedding, /config) is correctly guarded by get_admin_user making this a targeted omission. This vulnerability is fixed in 0.9.5.	5.3	More Details
CVE-2026-33584	Exposed Keycloak management service in the Arqit Symmetric Key Agreement Platform enables unauthorized access to sensitive debug information such as metrics and health data. This issue affects Symmetric Key Agreement Platform: before 26.03.	5.3	More Details
CVE-2026-34883	An issue was discovered in the Portrait Dell Color Management application before 3.7.0 for Dell monitors. On Windows, a symbolic link vulnerability allows a local low-privileged user to escalate privileges to Administrator. During installation, the software writes the file CCFLFamily_07Feb11.edr to C:\ProgramData\Portrait Displays\CW\data\i1D3\ while running with elevated privileges. Because the installer does not properly validate symbolic links or reparse points at the destination path, an attacker can create a malicious link that redirects the write operation to an arbitrary system location, enabling arbitrary file creation or overwrite with elevated privileges.	5.3	More Details
CVE-2026-7009	When curl is told to use the Certificate Status Request TLS extension, often referred to as *OCSP stapling*, to verify that the server certificate is valid, it fails to detect OCSP problems and instead wrongly consider the response as fine.	5.3	More Details
CVE-	Successfully using libcurl to do a transfer over a specific HTTP proxy (`proxyA`) with **Digest** authentication and then changing the		More

2026-7168	proxy host to a second one (`proxyB`) for a second transfer, reusing the same handle, makes libcurl wrongly pass on the `Proxy-Authorization:` header field meant for `proxyA`, to `proxyB`.	5.3	Details
CVE-2026-44248	Netty is an asynchronous, event-driven network application framework. Prior to 4.2.13.Final and 4.1.133.Final, the MQTT 5 header Properties section is parsed and buffered before any message size limit is applied. Specifically, in MqttDecoder, the decodeVariableHeader() method is called before the bytesRemainingBeforeVariableHeader > maxBytesInMessage check. The decodeVariableHeader() can call other methods which will call decodeProperties(). Effectively, Netty does not apply any limits to the size of the properties being decoded. Additionally, because MqttDecoder extends ReplayingDecoder, Netty will repeatedly re-parse the enormous Properties sections and buffer the bytes in memory, until the entire thing parses to completion. This can cause high resource usage in both CPU and memory. This vulnerability is fixed in 4.2.13.Final and 4.1.133.Final.	5.3	More Details
CVE-2026-38740	Foscam VD1 Video Doorbell before V5.3.13_1072 is vulnerable to Cleartext Transmission of Sensitive Information. The device transmits sensitive Session Description Protocol (SDP), including ICE credentials and candidates, in cleartext over network interfaces. An attacker with network visibility can intercept these credentials to hijack media streams or authenticate to Foscam's TURN/relay infrastructure to forward arbitrary traffic at the vendor's expense.	5.3	More Details
CVE-2026-31388	Improper Access Control vulnerability in Apache OFBiz in multi-tenant deployments. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	5.3	More Details
CVE-2026-44309	Gitsign is a keyless Sigstore to signing tool for Git commits with your a GitHub / OIDC identity. Prior to 0.16.0, gitsign verify and gitsign verify-tag re-encode commit/tag objects through go-git's EncodeWithoutSignature before checking the signature, instead of verifying against the raw git object bytes. For malformed objects with duplicate tree headers, git-core and go-git parse different trees: git-core uses the first, go-git uses the second. A signature crafted over the go-git-normalized form (second tree) passes gitsign verify while git-core resolves the commit to a completely different tree. This breaks the invariant that a verified signature, the commit semantics git-core presents to users, and the object hash logged in Rekor all refer to the same content. This vulnerability is fixed in 0.16.0.	5.3	More Details
CVE-2026-8535	Out of bounds read in Media in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted JPEG file. (Chromium security severity: High)	5.3	More Details
CVE-2026-44288	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs includes a minimal UTF-8 decoder that accepted overlong UTF-8 byte sequences and decoded them to their canonical characters instead of replacing them. An attacker who can provide protobuf binary data decoded through the affected UTF-8 path may be able to bypass application-level checks that inspect raw bytes before protobuf string decoding. For example, bytes that do not contain certain ASCII characters could decode to strings containing those characters. This vulnerability is fixed in 7.5.6 and 8.0.2.	5.3	More Details
CVE-2025-14755	The Cost Calculator Builder plugin for WordPress is vulnerable to Unauthenticated Price Manipulation and Insecure Direct Object Reference (IDOR) in all versions up to, and including, 4.0.1 only when used in combination with Cost Calculator Builder PRO. This is due to the ccb_woocommerce_payment AJAX action being registered via wp_ajax_nopriv, making it accessible to unauthenticated users, and the renderWooCommercePayment() function passing user-controlled data directly to CCBWooCheckout::init() without authorization checks. This makes it possible for unauthenticated attackers to add WooCommerce products to their cart with attacker-controlled prices.	5.3	More Details
CVE-2026-24711	Northern.tech CFEngine Enterprise before 3.21.8, 3.24.3, and 3.27.0 has Incorrect Access Control.	5.3	More Details
CVE-2026-41933	Vvveb before 1.0.8.3 contains a directory listing information disclosure vulnerability that allows unauthenticated attackers to enumerate files and directories by accessing multiple paths lacking proper index directives in .htaccess files. Attackers can access directories such as admin asset paths, plugins, themes, and media folders to view filenames, file sizes, modification timestamps, and unrendered admin templates containing sensitive route maps.	5.3	More Details
CVE-2025-9987	The Broadstreet plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.53.1 via the get_sponsored_meta() AJAX action. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract data from password protected and private business details.	5.3	More Details
CVE-2026-8546	Out of bounds read in GPU in Google Chrome on Mac and Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-34019	When Bidirectional Forwarding Detection (BFD) is configured in Static and Dynamic routing protocols, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to stop processing BFD packets and cause the configured routing protocol to fail over. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2026-8543	Out of bounds read in FileSystem in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-8541	Out of bounds read in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-42526	In the AWS Secrets Manager and SSM Parameter Store secrets backends of `apache-airflow-providers-amazon` prior to 9.28.0, the team-scoping logic could resolve a `conn_id` containing a `/` (e.g. `"my_team/conn"`) to the same path as another team's team-scoped secret when the caller had no team context. A privileged caller without team context could therefore retrieve another team's secret by crafting a colliding `conn_id`. Fixed in 9.28.0 by switching the team-scope separator to `--` and rejecting team-shaped `conn_id`s when team context is absent. Affects the experimental multi-tenant teams feature only. Users are recommended to upgrade to `apache-airflow-providers-amazon` 9.28.0, which fixes the issue.	5.3	More Details
CVE-2026-8538	Insufficient validation of untrusted input in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform a denial of service via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
	### Summary `qs.stringify` throws `TypeError` when called with `arrayFormat: 'comma'` and `encodeValuesOnly: true` on an array containing `null` or `undefined`. The throw is synchronous and not handled by any of qs's null-related options (`skipNulls`, `strictNullHandling`). ### Details In the comma + `encodeValuesOnly` branch, `lib/stringify.js:145` mapped the array through the raw		

CVE-2026-8723	encoder before joining: ```js obj = utils.maybeMap(obj, encoder); ``` `utils.encode` (`lib/utils.js:195`) reads `str.length` with no null guard, so a `null` or `undefined` element throws `TypeError`. `skipNulls` and `strictNullHandling` are both checked in the per-element loop below this line and never get a chance to run. Same class of bug as the filter-array path fixed in 0c180a4. The vulnerable shape of the comma + `encodeValuesOnly` branch was introduced in 4c4b23d ("encode comma values more consistently", PR #463, 2023-01-19), first released in v6.11.1. #### PoC ```js const qs = require('qs'); qs.stringify({ a: [null, 'b'] }, { arrayFormat: 'comma', encodeValuesOnly: true }); qs.stringify({ a: [undefined, 'b'] }, { arrayFormat: 'comma', encodeValuesOnly: true }); qs.stringify({ a: [null] }, { arrayFormat: 'comma', encodeValuesOnly: true }); // TypeError: Cannot read properties of null (reading 'length') // at encode (lib/utils.js:195:13) // at Object.maybeMap (lib/utils.js:322:37) // at stringify (lib/stringify.js:145:25) ``` #### Fix `lib/stringify.js:145`, applied in 21f80b3 on `main` and released as v6.15.2: ```diff - obj = utils.maybeMap(obj, encoder); + obj = utils.maybeMap(obj, function (v) { + return v == null ? v : encoder(v); + }); ``` `null` and `undefined` now pass through `maybeMap` unchanged and reach the `join(',')` step as-is. For `{ a: [null, 'b'] }` this produces `a=,b`, matching the non-`encodeValuesOnly` comma path (which already joins before encoding and produces `a=%2Cb` for the same input). Single-element `[null]` arrays still collapse via the existing `obj.join(',') || null` and remain subject to `skipNulls` / `strictNullHandling` in the main loop. ### Affected versions `>=6.11.1 <6.15.2` — fixed in v6.15.2. The vulnerable code shape was introduced in 4c4b23d and first shipped in v6.11.1. Earlier versions — including all of 6.7.x, 6.8.x, 6.9.x, 6.10.x, and 6.11.0 — implemented the comma + `encodeValuesOnly` path differently (joining before encoding) and are not affected. Empirically verified across released versions. ### Impact Application code that calls `qs.stringify` with both `arrayFormat: 'comma'` and `encodeValuesOnly: true` (both non-default) on input that may contain a `null` or `undefined` array element will throw synchronously instead of producing a query string. In a typical Node.js HTTP framework (Express, Fastify, Koa, hapi) the sync throw is caught by the framework's error boundary and the affected request returns a 500; the worker process does not exit and subsequent requests are unaffected. The "kills the worker process" framing applies only to call sites outside a request-handler error boundary (background jobs, startup paths, stream pipelines) or to deployments with framework error handling explicitly disabled. The vulnerable input is a `null` or `undefined` entry inside an array; this is reachable from JSON request bodies or from application code constructing arrays from user input, but not from standard HTML form submissions (which produce strings or omitted fields, not literal `null`).	5.3	More Details
CVE-2026-42592	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, FilterOutboundURL resolves the hostname, checks the resolved IPs against the private-address deny-list, and returns only the error. It discards the resolved addresses. Chromium later performs its own DNS resolution when it navigates to the URL. An attacker who controls DNS for a hostname with a short TTL returns a public IP on the first query (Gotenberg allows) and a private IP on the second query (Chromium connects to the attacker-chosen internal address). The CDP Fetch.requestPaused handler re-checks the URL but runs its own DNS resolution, leaving a timing window before Chromium's actual TCP connect. The rendered internal service response returns to the caller as a PDF. This vulnerability is fixed in 8.32.0.	5.3	More Details
CVE-2021-47934	MyBB Timeline Plugin 1.0 contains cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through thread titles, post content, and user profile fields like Location and Bio. Attackers can also exploit a cross-site request forgery vulnerability in the timeline.php profile action to change a user's cover picture by crafting malicious forms that execute when victims visit affected profiles.	5.3	More Details
CVE-2026-42593	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, pdfengines/merge, pdfengines/split, libreoffice/convert, chromium/convert/url, chromium/convert/html, and chromium/convert/markdown accept stampSource=pdf + stampExpression=/path and watermarkSource=pdf + watermarkExpression=/path from anonymous callers. The dedicated stamp/watermark routes require an uploaded file when the source type is image or pdf; these six routes only overwrite the expression when a file is uploaded, leaving the user-controlled path intact when no file is attached. pdfcpu opens the path and composites its pages onto the output PDF, which returns to the caller. An attacker reads any PDF the Gotenberg process can access on the container filesystem. This vulnerability is fixed in 8.32.0.	5.3	More Details
CVE-2026-40435	When configured, IP-based access restrictions for httpd do not cover all endpoints, which may allow connections from blocked addresses. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2018-25336	Joomla jCart for OpenCart 2.3.0.2 contains a cross-site request forgery vulnerability that allows attackers to modify user account information without authentication. Attackers can craft malicious HTML forms targeting endpoints , and to change user credentials, passwords, and affiliate account details when victims visit the attacker-controlled page.	5.3	More Details
CVE-2026-8516	Insufficient validation of untrusted input in DataTransfer in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Critical)	5.3	More Details
CVE-2026-8737	A weakness has been identified in Sanluan PublicCMS 5.202506.d. This issue affects the function execute of the file publiccms-trade/src/main/java/com/publiccms/views/directive/trade/TradeAddressListDirective.java of the component Trade Address Query Handler. Executing a manipulation of the argument userId/id can lead to missing authentication. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2018-25327	Joomla! Component Js Jobs 1.2.0 contains a cross-site request forgery vulnerability that allows attackers to perform state-changing actions without token validation. Attackers can craft malicious HTML forms targeting administrative endpoints like job.jobenforcedelete to delete job entries or modify component settings when administrators visit attacker-controlled pages.	5.3	More Details
CVE-2026-8739	A vulnerability was detected in Sanluan PublicCMS 5.202506.d. The affected element is the function getSignKey of the file publiccms-core/src/main/java/com/publiccms/logic/component/config/SafeConfigComponent.java. The manipulation of the argument privatefile_key results in use of hard-coded cryptographic key . The attack can be executed 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.	5.3	More Details
CVE-2026-42572	Hatchet is a platform for orchestrating background tasks, AI agents, and durable workflows at scale. Prior to 0.83.39, a missing authorization directive on the GET /api/v1/stable/dags/tasks endpoint caused Hatchet's tenant-membership check to be skipped for this route. A user authenticated to any tenant on the same Hatchet instance could query the endpoint with another tenant's UUID and a DAG UUID belonging to that tenant, and receive task metadata for that DAG. This vulnerability is fixed in 0.83.39.	5.3	More Details
CVE-2026-24000	Fleet is open source device management software. Prior to version 4.80.1, Fleet trusted client-supplied IP address headers when determining the source IP for incoming requests. This allowed authenticated and unauthenticated clients to spoof their apparent IP address and bypass per-IP rate limiting controls. Fleet determines a client’s public IP address using HTTP headers such as X-Forwarded-For, X-Real-IP, and/or True-Client-IP. These headers were trusted without validation. An attacker could supply arbitrary values in these headers, causing Fleet to treat each request as originating from a different IP address. This could allow an attacker to bypass per-IP rate limits and increase the effectiveness of brute-force or password-spraying attempts against authentication endpoints. This issue does not allow authentication bypass, privilege escalation, data exposure, or remote code execution on its own. Version 4.80.1 contains a patch. As a workaround, run Fleet behind a trusted reverse proxy or load balancer that overwrites client IP headers.	5.3	More Details

CVE-2025-14033	The ilGhera Support System for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_ticket_content_callback' function in all versions up to, and including, 1.3.0. This makes it possible for unauthenticated attackers to view any support ticket content, including sensitive customer information and private communications, by providing a ticket ID.	5.3	More Details
CVE-2026-8750	A vulnerability was identified in h2oai h2o-3 up to 7402. Affected by this issue is the function importFiles of the file h2o-core/src/main/java/water/persist/PersistNFS.java of the component ImportFile API. Such manipulation leads to information disclosure. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-64526	Strapi is an open source headless content management system. In Strapi versions prior to 5.45.0, the rate-limit middleware in the users-permissions plugin derived its rate-limit key in part from `ctx.request.body.email`, including on routes whose body schema does not contain an `email` field (`/auth/local`, `/auth/reset-password`, `/auth/change-password`). An unauthenticated attacker could include an arbitrary `email` value in the request body to obtain a fresh rate-limit key per request, effectively bypassing per-IP throttling on those routes and enabling high-volume credential brute-force, password-reset code brute-force, and credential-stuffing attempts. The rate-limit key was constructed as `${userIdentifier}:${requestPath}:${ctx.request.ip}`, where `userIdentifier = ctx.request.body.email`. On routes that legitimately use email as their identifier (e.g. `/auth/forgot-password`, `/auth/local/register`), this scoping is correct. On routes that use a different identifier (`identifier` for login, `code` for password reset, `currentPassword` for password change), the email field was not part of the route contract, but the middleware still incorporated it into the key, allowing a caller to rotate the value and obtain a unique key on every request. The patch in version 5.45.0 maintains an allow-list of routes that legitimately key on the email field and excludes that key component on every other route the middleware is mounted on. OAuth callback paths (`/connect/*`) are treated identifier-less. On routes outside the allow-list, the middleware now falls back to a fixed identifier-less key, ensuring per-IP throttling remains effective even when the request body is attacker-controlled.	5.3	More Details
CVE-2026-6206	The MW WP Form plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 5.1.2 via the _get_post_property_from_querystring() function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	5.3	More Details
CVE-2026-45205	Uncontrolled Recursion vulnerability in Apache Commons. When processing an untrusted configuration file, Commons Configuration will throw a StackOverflowError for YAML input with cycles. This issue affects Apache Commons: from 2.2 before 2.15.0. Users are recommended to upgrade to version 2.15.0, which fixes the issue.	5.3	More Details
CVE-2026-8582	Object lifecycle issue in Dawn in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-8752	A weakness has been identified in h2oai h2o-3 up to 7402. This vulnerability affects the function exec of the file h2o-core/src/main/java/water/rapids/ast/prims/misc/AstSetProperty.java of the component Rapids setproperty Primitive Handler. Executing a manipulation can lead to improper access controls. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-36438	An issue in Intelbras VIP-1230-D-G4 Version V2.800.00IB00C.0.T allows a remote attacker to obtain sensitive information via password reset functionality under /OutsideCmd	5.3	More Details
CVE-2026-45740	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.8 and 8.2.0, protobufjs could recurse without a depth limit while expanding nested JSON descriptors through Root.fromJSON() and Namespace.addJSON(). A crafted JSON descriptor with deeply nested namespace definitions could cause the JavaScript call stack to be exhausted during descriptor loading. This vulnerability is fixed in 7.5.8 and 8.2.0.	5.3	More Details
CVE-2026-44373	Nitro is a next generation server toolkit. Prior to 3.0.260429-beta, an attacker could bypass a proxy route rule by sending percent-encoded path traversal (..%2f) in the URL, causing Nitro to forward a request that the upstream resolved outside the configured scope. This vulnerability is fixed in 3.0.260429-beta.	5.3	More Details
CVE-2026-44379	MISP is an open source threat intelligence and sharing platform. Prior to 2.5.37, MISP Collections did not enforce RFC 4122 UUID validation on the uuid field. As a result, a user able to create or modify Collection records could submit malformed UUID values, potentially causing integrity issues or unexpected behaviour in code paths that assume Collection UUIDs are valid identifiers. This vulnerability is fixed in 2.5.37.	5.3	More Details
CVE-2026-44381	MISP is an open source threat intelligence and sharing platform. Prior to 2.5.37, a SQL injection vulnerability existed in the handling of user-controlled ordering parameters in the event and shadow attribute listing endpoints. The affected code accepted order or sort values from request parameters and incorporated them into database query ordering clauses without sufficient validation of the requested field name. An attacker with access to the affected endpoints could craft a malicious ordering parameter to manipulate the generated SQL query. Depending on database permissions and query context, this could potentially allow unauthorized access to data, modification of query behavior, or other database-level impact. This vulnerability is fixed in 2.5.37.	5.3	More Details
CVE-2026-44195	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.7, a logic flaw in the OPNsense lockout_handler allows an unauthenticated attacker to continuously reset the authentication failure counter for their IP address. By interjecting a crafted username containing a success keyword ("Accepted" or "Successful login") between normal brute-force attempts, an attacker can prevent the failure counter from ever reaching the lockout threshold. This vulnerability is fixed in 26.1.7.	5.3	More Details
CVE-2026-8454	Imager::File::GIF versions through 1.002 for Perl allow a heap out of bounds (OOB) write on crafted multi-frame GIF files. Imager::File::GIF's i_readgif_multi_low allocates a single per-row buffer GifRow sized for the GIF's global screen width 'SWidth' and reuses it across every image in the file. The page-match branch validates Image.Width + Image.Left > SWidth before each DGifGetLine write, but the parallel skip-image branch at imgif.c:790-805 calls DGifGetLine(GifFile, GifRow, Width) with no such check.	5.3	More Details
CVE-2026-32244	Discourse is an open-source discussion platform. In versions prior to 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1, outdated cached AI summaries can leak removed content to anonymous and unprivileged users who cannot regenerate summaries. This issue has been fixed in versions 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1. To work around this issue, restrict summary generation by tightening the allowed groups on the summarization Personas.	5.3	More Details
CVE-2026-44457	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.18, Cache Middleware does not skip caching for responses that declare per-user variance via Vary: Authorization or Vary: Cookie. As a result, a response cached for one authenticated user may be served to subsequent requests from different users. This vulnerability is fixed in 4.12.18.	5.3	More Details
	Crypt::Argon2 versions from 0.017 before 0.031 for Perl perform a heap out-of-bounds read in argon2_verify on empty encoded input.		

CVE-2026-8463	The auto-detect form of argon2_verify passes encoded_len - 1 as the length argument to memchr without checking that encoded_len is non-zero. When the encoded string is empty, the size_t subtraction underflows to SIZE_MAX and memchr scans adjacent heap memory looking for a '$' separator byte. A caller that invokes argon2_verify against a stored hash that may legitimately be empty (for example a placeholder row or a NULL column materialised as an empty string) reads out-of-bounds heap memory, which can crash the process or leak the position of an adjacent '$' byte into subsequent parsing.	5.3	More Details
CVE-2026-2515	The Hostinger Reach – AI-Powered Email Marketing for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'handle_ajax_action' function in all versions up to, and including, 1.3.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to use the 'hostinger_reach_connection_notice_action' action to update the API key value stored in the database. This vulnerability can only be exploited when the plugin is not connected to a site and no API key value exists in the database.	5.3	More Details
CVE-2026-8583	Insufficient policy enforcement in WebXR in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-31387	Improper Authentication vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	5.3	More Details
CVE-2026-8814	Versions of the package exifreader before 4.39.0 are vulnerable to Improper Handling of Highly Compressed Data (Data Amplification) due to decompressing PNG zTXt metadata without enforcing a built-in maximum decompressed output size. When asynchronous parsing is enabled, a crafted PNG file containing a highly compressed zTXt chunk can cause ExifReader to materialize a disproportionately large Comment value in memory.	5.3	More Details
CVE-2026-44294	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs generated JavaScript property accessors from schema-controlled field and oneof names. Certain control characters in field names were not escaped before being embedded into generated function bodies. A crafted schema or JSON descriptor could therefore cause generated encode, decode, verify, or conversion functions to fail during compilation. This vulnerability is fixed in 7.5.6 and 8.0.2.	5.3	More Details
CVE-2026-44431	urllib3 is an HTTP client library for Python. From 1.23 to before 2.7.0, cross-origin redirects followed from the low-level API via ProxyManager.connection_from_url().urlopen(..., assert_same_host=False) still forward these sensitive headers. This vulnerability is fixed in 2.7.0.	5.3	More Details
CVE-2026-6145	The User Registration & Membership plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 5.1.5. This is due to the is_admin_creation_process() method relying solely on the presence of action=createuser in the $_REQUEST superglobal without performing any authentication or capability check. This makes it possible for unauthenticated attackers to bypass the admin approval requirement when registering new accounts via the fallback submission path.	5.3	More Details
CVE-2026-44292	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.5.6 and 8.0.2, protobufjs generated message constructors copied enumerable properties from a provided properties object without filtering the __proto__ key. If an application constructed a message from an attacker-controlled plain object, an own enumerable __proto__ property could alter the prototype of that individual message instance. This vulnerability is fixed in 7.5.6 and 8.0.2.	5.3	More Details
CVE-2020-37241	bloofoxCMS 0.5.2.1 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions by tricking logged-in users into visiting malicious pages. Attackers can craft hidden forms targeting the admin user creation endpoint to add new administrative accounts with arbitrary credentials without requiring explicit user consent.	5.3	More Details
CVE-2026-8612	WWW::Mechanize::Cached versions before 2.00 for Perl deserialize cached HTTP responses from a world-writable on-disk cache, enabling local response forgery and code execution. With no explicit cache backend, WWW::Mechanize::Cached constructs a default Cache::FileCache under /tmp/FileCache without overriding the backend's documented directory_umask of 000, so the cache root and its subdirectories are created mode 0777 with no sticky bit. Cache entries are named by sha1_hex of the request and read back through Storable::thaw on the next cache hit. A local attacker with write access to the cache tree can replace a victim's cache entry for a known URL with an arbitrary frozen HTTP::Response blob, causing the victim's next get() of that URL to return attacker controlled response bytes. Because the bytes are passed to Storable::thaw, a victim process that has loaded any class with a side-effectful STORABLE_thaw, DESTROY, or overload hook can be escalated to arbitrary code execution.	5.3	More Details
CVE-2026-6429	When asked to both use a `.netrc` file for credentials and to follow HTTP redirects, libcurl could leak the password used for the first host to the followed-to host under certain circumstances.	5.3	More Details
CVE-2026-45248	Hedera Guardian through 3.5.1 contains an authentication bypass vulnerability in the GET /api/v1/demo/registered-users endpoint that allows unauthenticated attackers to retrieve sensitive user information. Attackers can access the endpoint without providing authentication credentials to obtain usernames, Hedera DIDs, parent registry DIDs, system roles, and policy role assignments for all registered users in the system.	5.3	More Details
CVE-2026-6965	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to and including 3.9.9. This is due to the `get_course_id_by()` function unconditionally trusting the user-supplied `course` GET parameter as the authoritative course ID for content ownership lookups, which is then consumed by `can_user_manage()`, the plugin's sole authorization gate for instructor-level operations, causing it to evaluate instructor membership against the attacker-controlled course rather than the course that actually owns the target content object. This makes it possible for authenticated attackers, with instructor-level access and above, to perform unauthorized operations on any other instructor's course content, including permanently deleting lessons, assignments, quizzes (with cascading deletion of all student attempt data), topics, announcements, and Q&A threads, as well as creating or modifying lessons, topics, and announcements in victim courses, manipulating student quiz grades, and reading unpublished lesson and quiz content.	5.3	More Details
CVE-2026-8681	The Essential Chat Support plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.0.1. 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 reset all plugin configuration settings — including general settings, display rules, custom CSS, and WooCommerce tab settings — to their defaults by sending a POST request with ecs_reset_settings=1.	5.3	More Details
CVE-2025-62308	HCL AION is affected by a vulnerability where sensitive backend infrastructure details may be exposed. Exposure of such information could reveal internal system architecture or configuration details, which may potentially assist in further analysis or targeted actions under certain conditions	5.1	More Details
CVE-	HCL AION is affected by a vulnerability where certain operations may trigger out-of-band interactions, potentially resulting in unintended		More

2025-62305	disclosure of sensitive information. Such behaviour may allow exposure of data to external systems under specific conditions.	5.1	Details
CVE-2026-44441	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.106.0 and 16.16.0, a malicious user could send a crafted request to an endpoint, which would lead to the server making an HTTP call to a service of the user's choice. This vulnerability is fixed in 15.106.0 and 16.16.0.	5.0	More Details
CVE-2026-41051	csync2 uses insecure temporary directories when compiled with C99 or later, allowing for TOCTOU style attacks on the temporary directories.	5.0	More Details
CVE-2026-8767	A vulnerability has been found in vercel ai up to 3.0.97. Impacted is the function run of the file .github/workflows/prettier-on-automerge.yml of the component PR Branch Name Interpolation. The manipulation leads to os command injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-33234	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. In versions 0.1.0 through 0.6.51, SendEmailBlock in autogpt_platform/backend/backend/blocks/email_block.py accepts a user-supplied smtp_server (string) and smtp_port (integer) as per-execution block inputs, then passes them directly to Python's smtplib.SMTP() to open a raw TCP connection with no IP address validation. This completely bypasses the platform's hardened SSRF protections in backend/util/request.py — the validate_url_host() function and BLOCKED_IP_NETWORKS blocklist that every other block uses to block connections to private, loopback, link-local, and cloud metadata addresses. An authenticated user on a shared AutoGPT deployment can use this to perform non-blind internal network port scanning and service fingerprinting: smtplib reads the target's TCP banner on connect and embeds it in the exception message, which is persisted as user-visible block output via the execution framework. This issue has been fixed in version 0.6.52.	5.0	More Details
CVE-2025-27852	The locally served web site on the Garmin WDU (v1 1.4.6 and v2 5.0) allows a reflected cross site scripting (XSS) attack. This allows an attacker on the local network segment to execute arbitrary JavaScript code within the context of the WDU webpage. Full administrator level access to the device is possible. To initiate an exploit of this vulnerability, the victim must execute two actions: (1) view a specific URL served by the WDU, and (2) click an element on the rendered page.	5.0	More Details
CVE-2026-44550	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, FolderForm uses model_config = ConfigDict(extra='allow'), which permits arbitrary fields to pass through Pydantic validation and be included in model_dump(exclude_unset=True). In insert_new_folder, the server-assigned user_id is placed at the start of the dict and then overwritten by the spread of form data. Because FolderModel declares user_id: str as a real field (not just a form extra), any attacker-supplied user_id in the POST body is accepted by the model and persisted on the Folder row. This vulnerability is fixed in 0.9.0.	5.0	More Details
CVE-2026-37978	A flaw was found in Keycloak. A low-privilege administrator with the 'view-clients' role can exploit this by invoking the 'evaluate-scopes' Admin API endpoints with an arbitrary user ID (userId) parameter. This vulnerability allows for cross-role personally identifiable information (PII) leakage, enabling unauthorized visibility into user identities and authorizations across the realm. Exploitation is possible remotely via network access to the Admin API.	4.9	More Details
CVE-2026-45054	CubeCart is an ecommerce software solution. Prior to 6.7.0, the admin orders-transactions listing page (admin.php?_g=orders&node=transactions) builds a raw ORDER BY SQL fragment from the attacker-controlled $_GET['sort'] array without column or direction validation. Both the column key and the direction value flow into the query string as bare SQL tokens, and the framework's sqlSafe() (mysqli escape_string) escapes only quote characters — none of which are required for ORDER BY injection. An authenticated administrator with the minimum CC_PERM_READ permission on orders can execute arbitrary SQL against the store database, including time-based blind extraction of admin password hashes, customer PII, and integrated payment-gateway credentials. This vulnerability is fixed in 6.7.0.	4.9	More Details
CVE-2026-7046	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'table' parameter in all versions up to, and including, 9.1.12 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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.	4.9	More Details
CVE-2026-42780	A directory traversal vulnerability exists in BIG-IP SSL Orchestrator that allows an authenticated attacker with high privilege to overwrite, delete or corrupt arbitrary local files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details
CVE-2026-42063	A vulnerability exists in iControl SOAP where an authenticated attacker with the Resource Administrator or Administrator role can download sensitive files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details
CVE-2026-41954	Sensitive information disclosure vulnerability exists in the undisclosed iControl REST endpoint and TMOS Shell (tmsh) command which may allow an authenticated attacker with resource administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details
CVE-2026-34246	CtrlPanel is open-source billing software for hosting providers. Versions 1.1.1 and prior contain a Stored Cross-Site Scripting (XSS) vulnerability exists in the admin role management interface. In app/Http/Controllers/Admin/RoleController.php, the datatable() method interpolates $role->name and $role->color directly into a element's HTML and style attribute without sanitization, and the chained .rawColumns(['actions', 'name']) call instructs DataTables to render the name column as raw HTML, bypassing automatic output escaping. An admin with role creation or edit permissions can inject a payload such as <img src=x onerror="alert('XSS_POC')"> into the name or color fields, which is persisted to the database and executes in the browser of every admin who loads the /admin/roles page. This enables session hijacking via cookie theft, credential harvesting through fake login prompts or keyloggers, lateral privilege escalation by performing admin actions on behalf of victims, and a persistent backdoor that re-executes on every page load until the malicious role record is removed. This issue has been resolved in version 1.2.0.	4.8	More Details
CVE-2026-39428	CubeCart is an ecommerce software solution. Prior to 6.6.0, a Stored Cross-Site Scripting (XSS) vulnerability exists in CubeCart v6.x. An attacker with administrative privileges can inject malicious JavaScript payloads into multiple fields during the creation or modification of a product. These payloads are stored in the database and executed whenever a user (customer or another administrator) views the affected product pages, which could lead to session hijacking or unauthorized actions. This vulnerability is fixed in 6.6.0.	4.8	More Details
CVE-2026-8367	aria2c accepts a server certificate with incorrect Extended Key Usage (EKU). If the attackers compromise a certificate (with the associated private key) issued for a different purpose, they may be able to reuse it for TLS server authentication.	4.8	More Details
	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_charset_module module. When charset, source_charset, and		

CVE-2026-42934	charset_map and proxy_pass with disabled buffering ("off") directives are configured, unauthenticated attackers can send requests that with conditions beyond the attackers' control to cause a heap buffer over-read in the NGINX worker process, leading to limited disclosure of memory or a restart. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.8	More Details
CVE-2026-40701	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_ssl_module module when the ssl_verify_client directive is set to "on" or "optional," and the ssl_ocsp directive is set to "on" or the leaf parameters are configured with a resolver. With this configuration, an unauthenticated attacker can send requests along with conditions beyond its control that may cause a heap-use-after-free error in the NGINX worker process. This vulnerability may result in limited modification of data or the NGINX worker process restarting. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.8	More Details
CVE-2026-44568	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the AccountPending.svelte component renders the admin-configured "Pending User Overlay Content" using marked.parse() inside {@html} with an incorrect DOMPurify application order. An admin can inject arbitrary JavaScript into the Pending User Overlay Content that executes in the browser context of any pending user who views the overlay page. This vulnerability is fixed in 0.9.0.	4.8	More Details
CVE-2026-8773	A security vulnerability has been detected in linlinjava litemall up to 1.8.0. Affected by this vulnerability is the function backup/load of the file litemall-db/src/main/java/org/linlinjava/litemall/db/util/DbUtil.java of the component Database Setting Handler. The manipulation of the argument db/password leads to argument injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-8565	Inappropriate implementation in Downloads in Google Chrome on Mac prior to 148.0.7778.168 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium)	4.7	More Details
CVE-2026-32848	NetBSD prior to commit ec8451e contains a race condition vulnerability in cryptodev_op() within the opencrypto subsystem that allows local attackers to trigger a double-free condition by concurrently issuing CIOCCRYPT operations on the same session identifier on SMP systems. Attackers can exploit mutable per-operation state embedded in the csession struct to corrupt kernel heap memory.	4.7	More Details
CVE-2026-8724	A security flaw has been discovered in Dataease 2.10.20. Impacted is the function SqlparserUtils.transFilter of the file SqlparserUtils.java of the component Data Dashboard. 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.	4.7	More Details
CVE-2026-44581	Next.js is a React framework for building full-stack web applications. From 13.4.0 to before 15.5.16 and 16.2.5, App Router applications that rely on CSP nonces can be vulnerable to stored cross-site scripting when deployed behind shared caches. In affected versions, malformed nonce values derived from request headers could be reflected into rendered HTML in an unsafe way, allowing an attacker to poison cached responses and cause script execution for later visitors. This vulnerability is fixed in 15.5.16 and 16.2.5.	4.7	More Details
CVE-2026-8772	A weakness has been identified in linlinjava litemall up to 1.8.0. Affected is an unknown function of the component Admin Endpoint. Executing a manipulation can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. Multiple endpoints are affected. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-44455	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.16, Improper handling of JSX element tag names in hono/jsx allowed unvalidated tag names to be directly inserted into the generated HTML output. When untrusted input is used as a tag name via the programmatic jsx() or createElement() APIs during server-side rendering, specially crafted values may break out of the intended element context and inject unintended HTML. This vulnerability is fixed in 4.12.16.	4.7	More Details
CVE-2026-44428	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.6, the client-side and server-side GitHub OIDC flow is bound only to a global audience string, not to the specific registry instance being targeted. On the client side, the publisher always appends audience=mcp-registry when requesting the GitHub Actions ID token, regardless of the selected --registry URL. On the server side, the exchange endpoint validates only that same fixed audience and then derives publish permissions directly from repository_owner. As a result, a token legitimately obtained while interacting with one registry deployment remains acceptable to any other deployment that shares the same code and audience string. This vulnerability is fixed in 1.7.6.	4.7	More Details
CVE-2026-44661	python-utcp is the python implementation of UTCP. Prior to 1.1.3, the utcp-http plugin is vulnerable to a blind Server-Side Request Forgery (SSRF) caused by a trust-boundary inconsistency between manual discovery and tool invocation. register_manual() validates the discovery URL against an HTTPS / loopback allowlist, but call_tool() and call_tool_streaming() reuse the resolved tool_call_template.url directly without revalidating, and the OpenAPI converter blindly trusts whatever servers[0].url an attacker-hosted spec declares. An attacker who hosts a malicious OpenAPI spec on a legitimate HTTPS endpoint can declare e.g. servers: [{ url: "http://127.0.0.1:9090" }] or servers: [{ url: "http://169.254.169.254" }]; the OpenAPI converter then produces tools whose URL points at internal services on the agent host. All three HTTP-class protocols (utcp_http.http, utcp_http.streamable_http, utcp_http.sse) shared the same gap. This vulnerability is fixed in 1.1.3.	4.7	More Details
CVE-2026-21789	HCL Connections contains a broken access control vulnerability that may allow unauthorized user to update data in certain scenarios.	4.6	More Details
CVE-2026-45317	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, an application-wide Cross-Site Request Forgery (CSRF) vulnerability was found Open-WebUI's image uploading functionality. An attacker can set an image URL to a malicious endpoint, allowing them to perform actions on behalf of a victim user. Any authenticated user can exploit this vulnerability, and any user who views the compromised image (e.g., a profile picture) will unknowingly send a GET request to the attacker-controlled URL. This can lead to cookie theft, denial of service (DoS), or other malicious actions. This vulnerability is fixed in 0.9.3.	4.6	More Details
CVE-2025-15645	Ledger Nano X, Flex, and Stax devices contain a denial of service vulnerability in the MCU firmware update process due to missing validation of the reset_handler parameter during firmware flashing. An attacker can provide a crafted reset_handler address pointing to invalid memory or attacker-controlled code to cause the device to enter an unrecoverable fault state during boot, resulting in permanent loss of operability.	4.6	More Details
CVE-2025-40900	An Angular template injection vulnerability was discovered in the Reports functionality due to improper validation of an input parameter. An authenticated user with report privileges can define a malicious report containing an Angular template payload, or a victim can be socially engineered to import a malicious report template. When the victim views or imports the report, the Angular template executes in their browser context, allowing the attacker to modify application data, or disrupt application availability. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	4.6	More Details
CVE-	Claude HUD through 0.0.12, patched in commit 234d9aa, constructs OSC 8 terminal hyperlink escape sequences using raw cwd and branchUrl values without stripping control characters or encoding embedded values, allowing attackers to inject arbitrary ANSI codes		

2026-47090	into terminal sessions. Attackers can embed ESC+backslash sequences in the current working directory or branch URL to execute malicious ANSI codes including text color changes, forged prompts, and OSC 52 clipboard writes, or trigger outbound HTTP requests to attacker-controlled remotes when hyperlinks are clicked.	4.6	More Details
CVE-2026-42549	Flight is an extensible micro-framework for PHP. Prior to 3.18.1, the make:controller CLI command calls mkdir(..., recursive: true) on a path built from the user-supplied controller name, before Nette's class-name validation runs. The class-file write is correctly rejected by Nette when the name contains /, but the recursive directory creation side effect is already committed — including directories located outside the project root through ../ traversal. This vulnerability is fixed in 3.18.1.	4.4	More Details
CVE-2026-45736	ws is an open source WebSocket client and server for Node.js. Prior to 8.20.1, the websocket.close() implementation is vulnerable to uninitialized memory disclosure when a TypedArray is passed as the reason argument. This vulnerability is fixed in 8.20.1.	4.4	More Details
CVE-2026-42408	When BIG-IP DNS is provisioned, a vulnerability exists in an undisclosed TMOS Shell (tmsh) command that may allow a highly privileged authenticated attacker to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.4	More Details
CVE-2025-9989	The Broadstreet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.53.1 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-2026-28758	When BIG-IP DNS is provisioned, a vulnerability exists in the gtm_add and bigip_add iControl REST commands that return the ssh-password parameter in cleartext in the iControl REST response and is also logged in the audit log. This may allow a highly privileged, authenticated attacker with access to the audit log to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	4.4	More Details
CVE-2026-8537	Insufficient policy enforcement in ViewTransitions in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-1338	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.10 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with developer-role permissions to delete protected container registry tags due to improper authorization checks.	4.3	More Details
CVE-2026-6339	Mattermost versions 11.5.x <= 11.5.1, 11.4.x <= 11.4.3 fail to validate the X-Requested-With header on the burn-on-read reveal endpoint which allows an authenticated channel member to force the reveal of a burn-on-read message without recipient consent via a crafted Markdown image tag.. Mattermost Advisory ID: MMSA-2026-00636	4.3	More Details
CVE-2026-45385	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, an IDOR vulnerability exists in the Channels feature of Open WebUI, allowing any channel member to modify messages sent by other members (including administrators) within the same channel. In the update_message_by_id function, for group or dm type channels, only the caller's membership in the channel is checked via the is_user_channel_member function, without verifying message ownership. This allows any channel member to modify messages sent by other members within the same channel. This vulnerability is fixed in 0.9.5.	4.3	More Details
CVE-2018-25321	TP-Link TL-WR720N wireless router contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized administrative actions by crafting malicious web requests. Attackers can modify port forwarding rules via VirtualServerRpm.htm or change WiFi security settings via WlanSecurityRpm.htm by tricking authenticated users into visiting attacker-controlled pages.	4.3	More Details
CVE-2026-8729	A vulnerability was detected in Open5GS up to 2.7.7. This affects an unknown function in the library /lib/sbi/message.c of the component NRF. Performing a manipulation of the argument service-names/snssais results in denial of service. The attack is possible to be carried out remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-45147	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, POST /api/tag/getTag is registered with model.CheckAuth only, omitting both model.CheckAdminRole and model.CheckReadonly, despite the handler performing a configuration write that is normally guarded by both. Any authenticated user — including publish-service RoleReader accounts and RoleEditor accounts on a read-only workspace — can call this endpoint with a sort argument to mutate model.Conf.Tag.Sort and trigger model.Conf.Save(), which atomically rewrites the entire workspace conf.json. This vulnerability is fixed in 3.7.0.	4.3	More Details
CVE-2026-8746	A security flaw has been discovered in Open5GS up to 2.7.7. Affected by this issue is the function discover_handler in the library /lib/sbi/nghttp2-server.c of the component NRF. The manipulation results in use after free. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-8745	A vulnerability was identified in Open5GS up to 2.7.7. Affected by this vulnerability is the function ogs_timer_add in the library /src/ausf/nausf-handler.c of the component AUSF. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-8730	A flaw has been found in Open5GS up to 2.7.6. This impacts the function ogs_sbi_nf_instance_set_id in the library /lib/sbi/context.c of the component NRF. Executing a manipulation of the argument nfInstanceId can lead to denial of service. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-45148	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, broken access control in the searchAsset, searchTag, searchWidget, and searchTemplate publish-mode Readers can enumerate metadata from documents that are invisible to the publish service. This vulnerability is fixed in 3.7.0.	4.3	More Details
CVE-2026-45448	CWE-601 URL redirection to untrusted site ('open redirect')	4.3	More Details
CVE-2026-42058	An authenticated attacker's undisclosed requests to BIG-IP iControl REST can lead to an information leak of BIG-IP local user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.3	More Details

CVE-2026-8528	Insufficient validation of untrusted input in SiteIsolation in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass Site Isolation via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-8731	A vulnerability has been found in Open5GS up to 2.7.7. Affected is the function ogs_sbi_client_add in the library /lib/sbi/client.c of the component NRF. The manipulation of the argument client_pool leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-8728	A security vulnerability has been detected in Open5GS up to 2.7.7. The impacted element is the function ogs_sbi_discovery_option_parse_plmn_list in the library /lib/sbi/conv.c of the component NRF. Such manipulation of the argument target-plmn-list leads to denial of service. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-8744	A vulnerability was determined in Open5GS up to 2.7.7. Affected is the function ogs_sbi_subscription_data_add/ogs_sbi_nf_service_add in the library /lib/sbi/context.c of the component NRF. Executing a manipulation can lead to denial of service. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 819db11a08b9736a3576c4f99ceb28f7eb99523a. A patch should be applied to remediate this issue.	4.3	More Details
CVE-2026-44501	DataHub is an open-source metadata platform. Prior to 1.5.0.3, The DataHub frontend (datahub-frontend-react) deserializes attacker-controlled Java objects from the REDIRECT_URL HTTP cookie during the OIDC callback flow, with no integrity protection (no HMAC, no encryption). This is a Deserialization of Untrusted Data vulnerability (CWE-502) affecting the GET /callback/oidc endpoint. Successful exploitation requires a valid user account in the configured OIDC identity provider This vulnerability is fixed in 1.5.0.3.	4.3	More Details
CVE-2025-62311	HCL AION is affected by a vulnerability where backend service details may be transmitted over insecure HTTP channels. This may expose sensitive information to potential interception or unauthorized access during transmission under certain conditions	4.3	More Details
CVE-2026-6474	Externally-controlled format string in PostgreSQL timeofday() function allows an attacker to retrieve portions of server memory, via crafted timezone zones. Versions before PostgreSQL 18.4, 17.10, 16.14, 15.18, and 14.23 are affected.	4.3	More Details
CVE-2026-2325	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to limit the size of the request body on the start meeting API endpoint, which allows an authenticated attacker to cause resource exhaustion or denial of service via a crafted oversized HTTP POST request to {{/api/v1/meetings}}.. Mattermost Advisory ID: MMSA-2026-00608	4.3	More Details
CVE-2026-28759	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to validate that a remote cluster has access to a channel before processing membership removal requests during shared channel membership sync, which allows a malicious remote cluster to remove any user from any channel, including private channels, via crafted membership sync messages targeting channels the remote cluster is not authorized to access. Mattermost Advisory ID: MMSA-2026-00576	4.3	More Details
CVE-2026-3607	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.3 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with developer-role permissions to bypass package protection rules due to improper access control.	4.3	More Details
CVE-2026-6063	GitLab has remediated an issue in GitLab EE affecting all versions from 11.10 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that under certain conditions could have allowed an authenticated user with developer-role permissions to remove code owner approval rules from merge requests due to improper access control.	4.3	More Details
CVE-2026-8202	Using a densely populated chars mask and a large input string in the MongoDB aggregation operators $trim, $ltrim, and $rtrim, an authenticated user with aggregation permissions can pin CPU utilization at 100% for an extended period of time. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	4.3	More Details
CVE-2026-8144	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.1 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with project membership to enumerate private group members due to missing authorization checks.	4.3	More Details
CVE-2026-8783	A security vulnerability has been detected in omec-project amf up to 2.1.3-dev. This impacts the function UERadioCapabilityCheckResponse of the file ngap/dispatcher.go. Such manipulation leads to null pointer dereference. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2.2.0 will fix this issue. Upgrading the affected component is advised. The same pull request fixes multiple security issues.	4.3	More Details
CVE-2026-8782	A weakness has been identified in omec-project amf up to 2.1.3-dev. This affects an unknown function of the file ngap/handler.go of the component NGAP Message Handler. This manipulation causes null pointer dereference. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.2.0 mitigates this issue. It is recommended to upgrade the affected component. The same pull request fixes multiple security issues.	4.3	More Details
CVE-2026-8781	A security flaw has been discovered in omec-project amf up to 2.1.3-dev. The impacted element is the function RANConfiguration of the file ngap/handler.go. The manipulation results in null pointer dereference. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.2.0 is sufficient to resolve this issue. Upgrading the affected component is recommended. The same pull request fixes multiple security issues.	4.3	More Details
CVE-2026-8780	A vulnerability was identified in omec-project amf up to 2.1.3-dev. The affected element is an unknown function of the file ngap/dispatcher.go of the component NGAP Message Handler. The manipulation leads to memory corruption. The attack may be initiated remotely. The exploit is publicly available and might be used. Upgrading to version 2.2.0 is sufficient to fix this issue. It is suggested to upgrade the affected component. The same pull request fixes multiple security issues.	4.3	More Details
CVE-2026-8779	A vulnerability was determined in omec-project amf up to 2.1.3-dev. Impacted is the function NGSetupRequest of the file ngap/handler.go. Executing a manipulation of the argument InformationElement can lead to memory corruption. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.2.0 is recommended to address this issue. The affected component should be upgraded. The same pull request fixes multiple security issues.	4.3	More Details
CVE-2026-5365	The LatePoint plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 5.3.2. This is due to missing nonce verification on the request_cancellation() function. This makes it possible for unauthenticated attackers to cancel a logged-in customer's bookings via a forged request, granted they can trick the customer into performing an action such as clicking on a link.	4.3	More Details

CVE-2026-6340	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to validate 7zip archive structure before processing which allows an authenticated attacker to cause server memory exhaustion and denial of service via uploading a specially crafted 7zip file with excessive folder declarations.. Mattermost Advisory ID: MMSA-2026-00573	4.3	More Details
CVE-2018-25337	Joomla JoomOCShop 1.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions on behalf of authenticated users. Attackers can craft malicious HTML forms targeting account endpoints like /joomoc2/?route=account/edit and to modify user information or reset passwords without user consent.	4.3	More Details
CVE-2026-6575	Buffer over-read in PostgreSQL function pg_restore_attribute_stats() accepts array values of unmatched length, which causes query planning to read past end of one array. This allows a table maintainer to infer memory values past that array end. Within major version 18, minor versions before PostgreSQL 18.4 are affected. Versions before PostgreSQL 18 are unaffected.	4.3	More Details
CVE-2026-8769	A vulnerability was determined in vercel ai up to 3.0.97. The impacted element is the function createJsonResponseHandler/createJsonErrorResponseHandler of the file packages/provider-utils/src/response-handler.ts of the component provider-utils. This manipulation causes resource consumption. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6341	Mattermost Plugins versions <=11.5 11.1.5 10.13.11 11.3.4.0 fail to have API-level checks on which groups the user can create issues or attach comments to which allows a user that is member of multiple groups to create issues to a locked group via direct API requests. Mattermost Advisory ID: MMSA-2026-00602	4.3	More Details
CVE-2026-8766	A flaw has been found in Kilo-Org kilocode up to 7.0.47. This issue affects the function Load of the file packages/opencode/src/config/config.ts of the component Environment Variable Handler. Executing a manipulation of the argument KILO_CONFIG_CONTENT can lead to information disclosure. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-8765	A vulnerability was detected in Kilo-Org kilocode up to 7.0.47. This vulnerability affects the function Bun.file of the file packages/opencode/src/kilocode/review/worktree-diff.ts of the component File Diff API Endpoint. Performing a manipulation of the argument File results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6342	Mattermost Plugins versions <=11.5 11.1.5 10.13.11 11.3.4.0 fail to appropriately check for valid namespaces which allows plugin users to create subscriptions to groups that were not whitelisted via creating groups that share the same prefix as a whitelisted group. Mattermost Advisory ID: MMSA-2026-00601	4.3	More Details
CVE-2026-3074	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.7 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an unauthenticated user to download private debugging symbols from inaccessible projects due to improper access control.	4.3	More Details
CVE-2026-28732	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 Fail to enforce slash command trigger-word uniqueness during command updates which allows an authenticated team member with Manage Own Slash Commands permission to hijack and impersonate existing system or custom slash commands via editing their own slash command trigger to an already-registered trigger through the command update API. Mattermost Advisory ID: MMSA-2026-00597	4.3	More Details
CVE-2026-3073	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.6 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with developer-role permissions to bypass PyPI package protection rules and upload restricted packages due to improper authorization checks.	4.3	More Details
CVE-2026-44374	Backstage is an open framework for building developer portals. Prior to 0.6.11, the unprocessed entities read endpoints in @backstage/plugin-catalog-backend-module-unprocessed do not enforce permission authorization checks. Any authenticated user can access unprocessed entity records regardless of ownership. This is an information disclosure vulnerability affecting Backstage installations using this module. This is patched in @backstage/plugin-catalog-backend-module-unprocessed version 0.6.11, @backstage/plugin-catalog-unprocessed-entities-common version 0.0.15 and @backstage/plugin-catalog-unprocessed-entities version 0.2.30.	4.3	More Details
CVE-2026-6343	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to check public/private permissions which allows members without these permissions to access public playbooks via /get.. Mattermost Advisory ID: MMSA-2026-00591	4.3	More Details
CVE-2025-9988	The Broadstreet plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the create_advertiser AJAX action in all versions up to, and including, 1.53.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create advertisers.	4.3	More Details
CVE-2026-8552	Heap buffer overflow in GPU in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-3637	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 fail to check the create_post channel permission during post edit operations which allows an authenticated attacker with revoked posting privileges to modify their existing posts via direct API requests to the post update and patch endpoints.. Mattermost Advisory ID: MMSA-2026-00627	4.3	More Details
CVE-2026-37981	A flaw was found in Keycloak. A broken access control vulnerability in the Account Resources user lookup endpoint allows a remote authenticated user, who owns at least one User-Managed Access (UMA) resource, to enumerate and harvest personally identifiable information (PII) for all realm users. By sending crafted requests with arbitrary usernames or email values, the endpoint returns full profile objects for unrelated users. This leads to broad profile-level information disclosure.	4.3	More Details
CVE-2026-45007	phpMyFAQ before 4.1.2 contains missing permission checks in ConfigurationTabController.php where 12 endpoints use userIsAuthenticated() instead of userHasPermission(CONFIGURATION_EDIT). Any authenticated user can enumerate system configuration metadata including permission model, cache backend, mail provider, and translation provider by querying /admin/api/configuration endpoints, violating least privilege access control.	4.3	More Details
CVE-2026-7648	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to payment bypass through user-controlled key in all versions up to, and including, 4.3.5. This is due to improper handling of user-supplied request parameters in the REST API endpoint, which passes the unsanitized parameter array to the add_to_cart() function where array_merge() allows attacker-controlled values to overwrite hardcoded defaults. This makes it possible for authenticated attackers, with subscriber-level access and above, to enroll in any paid course entirely free of charge by supplying a quantity value of zero, which causes the order total to calculate as $0 and bypasses all payment gateway requirements.	4.3	More Details

CVE-2026-7525	The My Calendar – Accessible Event Manager plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.7.9. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with custom-level access and above, to bypass the moderation and approval workflow by tampering with the POST body to publish events or set other unauthorized statuses such as cancelled or private, in ways their role does not permit. While the UI correctly restricts low-privilege users to a draft-only submit button, this restriction is enforced only client-side, making it trivially bypassable by directly manipulating the POST request.	4.3	More Details
CVE-2026-44919	In OpenStack Ironic through 35.x before a3f6d73, during image handling, an infinite loop in checksum calculations can occur via the file:///dev/zero URL.	4.3	More Details
CVE-2026-44458	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.18, the JSX renderer escapes style attribute object values for HTML but not for CSS. Untrusted input in a style object value or property name can therefore inject additional CSS declarations into the rendered style attribute. The impact is limited to CSS and does not allow JavaScript execution or HTML attribute breakout. This vulnerability is fixed in 4.12.18.	4.3	More Details
CVE-2026-8802	A vulnerability was detected in opensourcepos Open Source Point of Sale up to 3.4.2. This issue affects the function getPicThumb of the file app/Controllers/Items.php. The manipulation of the argument pic_filename results in path traversal. The attack may be launched remotely. The patch is identified as def0c27a0e252668df8d942fc31e16d1edfd7323. A patch should be applied to remediate this issue. The vendor was contacted early about this disclosure.	4.3	More Details
CVE-2026-3426	The RTMKit Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the save_widget() and reset_all_widgets() functions in all versions up to, and including, 2.0.2. This makes it possible for authenticated attackers, with Author-level access and above, to modify or reset site-wide widget configurations.	4.3	More Details
CVE-2026-45009	phpMyFAQ before 4.1.2 contains an insufficient authorization vulnerability in admin-api routes that allows authenticated ordinary users to access administrative endpoints by only checking login status instead of verifying backend privileges. Attackers with valid frontend user accounts can access sensitive backend operational information including dashboard versions, LDAP configuration, Elasticsearch statistics, and health-check data.	4.3	More Details
CVE-2021-47958	CouchCMS 2.2.1 contains a server-side request forgery vulnerability that allows authenticated attackers to make arbitrary HTTP requests by uploading malicious SVG files. Attackers can upload SVG files containing external entity references through the browse.php endpoint to access internal services and resources.	4.3	More Details
CVE-2025-13874	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.1 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with Guest permissions to view issues in projects they were not authorized to access.	4.3	More Details
CVE-2025-4202	The Multicollab: Content Team Collaboration and Editorial Workflow plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'cf_add_comment' function in all versions up to, and including, 5.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add comments to arbitrary collaborations.	4.3	More Details
CVE-2026-28374	Editors could delete any annotation, even those they do not have read access to. The editor user cannot create or read the annotations.	4.3	More Details
CVE-2026-8830	A flaw was found in Keycloak. An authenticated user can bypass configured WebAuthn policies during credential registration by manipulating client-side JavaScript. This occurs because the server-side processAction() fails to validate that the newly created credential's parameters, such as public key algorithms, match the realm's configured WebAuthn policies. This could lead to the creation of credentials that do not adhere to administrative security requirements, potentially weakening the overall security posture of the system by allowing non-compliant authentication methods.	4.3	More Details
CVE-2020-37217	Easy2Pilot 7 contains a cross-site request forgery vulnerability that allows attackers to add unauthorized user accounts by tricking authenticated administrators into visiting malicious pages. Attackers can craft HTML forms targeting the admin.php?action=add_user endpoint with POST requests containing username and password parameters to create new administrative accounts without explicit user consent.	4.3	More Details
CVE-2026-45347	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.5.11, there is a blind server side request forgery (SSRF) via the PDF generate function. In the PDF export, user inputs are interpreted as HTML and embedded into the PDF. According to tests, scripts and some potentially dangerous tags (iFrame, Object, etc.) are blocked, preventing server-side content from being read through this vulnerability. However, an image tag can be used to force a server-side request (SSRF), as shown in the following below. This vulnerability is fixed in 0.5.11.	4.3	More Details
CVE-2026-7563	The Classified Listing – AI-Powered Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 5.3.10. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to add arbitrary notes to any order and trigger unsolicited notification and moderation emails to listing owners without administrative authorization.	4.3	More Details
CVE-2026-8425	The Notify Odoo plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the _updateSettings function. This makes it possible for unauthenticated attackers to change the Notify Odoo URL to an attacker-controlled URL and modify notification, tracking image, and allowed IP address 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-2026-45442	Missing Authorization vulnerability in Brainstorm Force Presto Player allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Presto Player: from n/a through 4.1.3.	4.3	More Details
CVE-2026-4607	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.9.8.4. This is due to the plugin not properly verifying that a user is authorized to perform an action via the pm_set_group_order, pm_set_group_items, and pm_set_field_order AJAX actions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify site-wide ProfileGrid group settings including group menu order, group list order, group icon display, and field ordering.	4.3	More Details
CVE-2026-8566	Insufficient policy enforcement in Payments in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE-2026-45387	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, when setting model permissions so that a group has read access to it, intending for other users to use it, those users also can read the model's system prompt. However users may consider their system prompt confidential, so this is considered a security issue. This vulnerability is fixed in 0.9.5.	4.3	More Details
CVE-2026-8559	Integer overflow in Internationalization in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-8560	Heap buffer overflow in SwiftShader in Google Chrome on Mac and iOS prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-4054	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3 Fail to validate the response body of proxied images, which allows a remote attacker to enact client-side DoS via an SVG file served from an attacker-controlled origin under a non-SVG Content-Type header (e.g. image/png) embedded in an og:image meta tag or Markdown image link.. Mattermost Advisory ID: MMSA-2026-00630	4.3	More Details
CVE-2026-8562	Side-channel information leakage in Navigation in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-44557	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the _validate_collection_access function uses an incomplete allowlist that only enforces ownership checks for collections matching user-memory-* and file-* patterns. All other collection names pass through unchecked — including the system-level knowledge-bases meta-collection, which stores the IDs, names, and descriptions of every knowledge base on the instance. Any authenticated user can query this meta-collection directly via the retrieval query endpoints to obtain a global index of all knowledge bases across all users. This vulnerability is fixed in 0.9.0.	4.3	More Details
CVE-2026-8563	Insufficient policy enforcement in IFrame Sandbox in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-8576	Inappropriate implementation in CORS in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-45386	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, Pin/Unpin is a write operation (modifies the message's is_pinned , pinned_by, pinned_at fields), but in standard channels it only checks read permission, allowing users with read-only access to pin/unpin any message. This vulnerability is fixed in 0.9.5.	4.3	More Details
CVE-2026-8567	Integer overflow in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-44559	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the GET /api/v1/channels/{id}/members endpoint only checks membership for group and dm channel types (lines 467-469). For standard channels — including private ones — there is no channel_has_access check before returning the member list. Any authenticated user who knows a private channel's UUID can enumerate all users with access to that channel. This vulnerability is fixed in 0.9.0.	4.3	More Details
CVE-2026-8564	Incorrect security UI in Downloads in Google Chrome on Android and Mac prior to 148.0.7778.168 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2026-8584	Inappropriate implementation in Views in Google Chrome on iOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2026-8784	A vulnerability was detected in npitre cramfs-tools up to 2.2. Affected is the function change_file_status of the file cramfsck.c. Performing a manipulation results in symlink following. The attack requires a local approach. The exploit is now public and may be used. The patch is named b4a3a695c9873f824907bd15659f2a6ac7667b4f. It is recommended to apply a patch to fix this issue.	4.2	More Details
CVE-2026-8736	A security flaw has been discovered in Oinone Pamirs up to 7.2.0. This vulnerability affects the function request.getParameter of the file LocalFileClient.java of the component RestController. Performing a manipulation of the argument uniqueFileName results in path traversal. The attack may be carried out on the physical device. 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.	4.1	More Details
CVE-2026-46470	An issue was discovered in GStreamer gst-plugins-good before 1.28.2. When parsing MP4 audio tracks, the isomp4 plugin's qtdemux_audio_caps function does not sufficiently validate atom data before performing division operations, leading to denial of service due to integer division by zero.	4.0	More Details
CVE-2026-46469	An issue was discovered in GStreamer gst-plugins-good before 1.28.2. When parsing MP4 audio tracks, the isomp4 plugin's qtdemux_parse_trak function does not sufficiently validate atom data before performing division operations, leading to denial of service due to integer division by zero.	4.0	More Details
CVE-2026-44430	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.7, the Registry's HTTP-based namespace verification (POST /v0/auth/http, POST /v0.1/auth/http) uses safeDialContext (internal/api/handlers/v0/auth/http.go:67-110) to refuse dialling private/internal addresses when fetching the well-known public-key file from a publisher-supplied domain. The blocklist (isBlockedIP, lines 125-133) relies entirely on Go stdlib's IsLoopback / IsPrivate / IsLinkLocalUnicast / IsMulticast / IsUnspecified plus a manual CGNAT range. None of these cover IPv6 6to4 (2002::/16), NAT64 (64:ff9b::/96 and 64:ff9b:1::/48 per RFC 8215), or deprecated site-local (fec0::/10) — all of which encode arbitrary IPv4 in the address bits and tunnel to RFC1918 / cloud-metadata services on dual-stack / NAT64-enabled hosts. This vulnerability is fixed in 1.7.7.	4.0	More Details
CVE-2026-27964	FacturaScripts is an open source accounting and invoicing software. Versions 2025.7 and prior contain a Reflected Cross-Site Scripting (XSS) vulnerability through the fsNick cookie parameter. The application reflects the cookie's value directly into the HTML without sanitization. The fsNick cookie is rendered into the DOM without encoding. While the server does reject the modified session and forces a logout, the HTML containing the payload reaches the browser first. This lets the script execute immediately upon load, effectively	3.9	More Details

	beating the redirect. This issue has been fixed in version 2025.8.		
CVE-2026-33585	Improper management of the idle timeout parameter in the Keycloak interface of the Arqit SKA-Platform enables an attacker to impersonate an authenticated tenant user via an unexpired browser session. This issue affects Symmetric Key Agreement Platform: before 26.03.	3.8	More Details
CVE-2026-3495	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to escape some variables that could contain malicious content during error page composition which allows an attacker with access to edit some site configuration to execute some malicious code via injecting some JS as part of those values.. Mattermost Advisory ID: MMSA-2026-00622	3.8	More Details
CVE-2026-44459	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.18, improper validation of the JWT NumericDate claims exp, nbf, and iat in hono/utils/jwt allows tokens with non-spec-compliant claim values to silently bypass time-based checks. This issue is not exploitable by an anonymous attacker; it only manifests when a malformed claim value reaches verify() — typically when the application itself issues such tokens, or when the signing key is otherwise under attacker control. This vulnerability is fixed in 4.12.18.	3.8	More Details
CVE-2026-6923	A side-channel attack, which requires a physical presence to the TPM, can lead to extraction of an Elliptic Curve Diffie-Hellman (ECDH) key.	3.8	More Details
CVE-2026-44572	Next.js is a React framework for building full-stack web applications. From 12.2.0 to before 15.5.16 and 16.2.5, an external client could send a x-nextjs-data header on a normal request to a path handled by middleware that returns a redirect. When that happened, the middleware/proxy could treat the request as a data request and replace the standard Location redirect header with the internal x-nextjs-redirect header. Browsers do not follow x-nextjs-redirect, so the response became an unusable redirect for normal clients. If the application was deployed behind a CDN or reverse proxy that caches 3xx responses without varying on this header, a single attacker request could poison the cached redirect response for the affected path. Subsequent visitors could then receive a cached redirect response without a Location header, causing a denial of service for that redirect path until the cache entry expired or was purged. This vulnerability is fixed in 15.5.16 and 16.2.5.	3.7	More Details
CVE-2026-6638	SQL injection in PostgreSQL logical replication ALTER SUBSCRIPTION ... REFRESH PUBLICATION allows a subscriber table creator to execute arbitrary SQL with the subscription's publication-side credentials. The attack takes effect at the next REFRESH PUBLICATION. Within major versions 16, 17, and 18, minor versions before PostgreSQL 18.4, 17.10, and 16.14 are affected. Versions before PostgreSQL 16 are unaffected.	3.7	More Details
CVE-2026-4273	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to validate that the RefreshedToken differs from the original invite token during remote cluster invite confirmation which allows an authenticated attacker to bypass token rotation and reuse the original invite token via sending a crafted invite confirmation with a RefreshedToken matching the original token. Mattermost Advisory ID: MMSA-2026-00575	3.7	More Details
CVE-2026-44582	Next.js is a React framework for building full-stack web applications. From 13.4.6 to before 15.5.16 and 16.2.5, React Server Component responses can be vulnerable to cache poisoning in deployments that rely on shared caches with insufficient response partitioning. In affected conditions, collisions in the _rsc cache-busting value can allow an attacker to poison cache entries so users receive the wrong response variant for a given URL. This vulnerability is fixed in 15.5.16 and 16.2.5.	3.7	More Details
CVE-2026-8803	A flaw has been found in opensourcepos Open Source Point of Sale up to 3.4.2. Impacted is the function Login of the file app/Models/Employee.php of the component Employee Login. This manipulation causes use of weak hash. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is considered difficult. The actual existence of this vulnerability is currently in question. The vendor explains: "[T]he code is still there to allow the upgrade path to work. The default password is initially seeded with the old hash function, but then migrated to a newer one after login. [T]he hash version check might be cleaned up in the future. Currently it's not actively in use as any password change will use a newer hash function."	3.7	More Details
CVE-2026-44589	Nuxt OG Image generates OG Images with Vue templates in Nuxt. The isBlockedUrl() denylist introduced in nuxt-og-image@6.2.5 to remediate GHSA-pqhr-mp3f-hrpp (Dmitry Prokhorov / Positive Technologies, March 2026) is incomplete. It has an incomplete IPv6 prefix list and is missing redirect re-validation. This vulnerability is fixed in 6.4.9.	3.7	More Details
CVE-2026-46483	Vim is an open source, command line text editor. Prior to 9.2.0479, a command injection vulnerability exists in tar#Vimuntar() in runtime/autoload/tar.vim when decompressing .tgz archives on Unix-like systems. The function builds :!gunzip and :!gzip -d commands using shellescape(tartail) without the {special} flag, allowing a crafted archive filename to trigger Vim cmdline-special expansion and execute shell commands in the user's context. This vulnerability is fixed in 9.2.0479.	3.6	More Details
CVE-2026-41962	Permission control vulnerability in the app management and control module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	3.6	More Details
CVE-2026-45316	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, the POST /api/v1/notes/{id}/pin endpoint performs a write operation (toggling the is_pinned field) but only checks for read permission. Users with read-only access to a shared note can pin/unpin it, which is a state-modifying action that should require write permission. This vulnerability is fixed in 0.9.3.	3.5	More Details
CVE-2026-7471	GitLab has remediated an issue in GitLab EE affecting all versions from 18.8 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user with control of a virtual registry upstream to make requests to internal hosts due to improper validation.	3.5	More Details
CVE-2026-4643	Mattermost Desktop App versions <=6.1 6.0.1 5.4.13.0 fail to prevent server-rendered content from closing an underlying application view in the Mattermost Desktop App which allows a malicious server or plugin to crash the desktop client via invoking {{window.close()}} in the renderer context, leading to a denial of service condition at the client level. Mattermost Advisory ID: MMSA-2026-00633	3.5	More Details
CVE-2026-45803	`gh` is GitHub's official command line tool. From 1.6.0 to before 2.92.0, a security vulnerability has been identified in GitHub CLI that could allow terminal escape sequence injection when users view GitHub Actions workflow logs using gh run view --log or gh run view --log-failed. The vulnerability stems from the way GitHub CLI handles raw Actions log output. The gh run view --log and gh run view --log-failed commands stream workflow log lines to stdout or the configured pager without sanitizing terminal control sequences. An attacker who can influence GitHub Actions log content, for example via a PR triggered workflow, can embed escape sequences that are replayed in the user's terminal when they inspect the run. Depending on the victim's terminal emulator, injected sequences could change the window title, manipulate on screen content, or in some terminal emulators (such as screen) potentially execute arbitrary commands. This vulnerability is fixed in 2.92.0.	3.5	More Details

CVE-2026-6333	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to validate the Host header when constructing response URLs for custom slash commands which allows an authenticated attacker to redirect slash command responses to an attacker-controlled server via a spoofed Host header.. Mattermost Advisory ID: MMSA-2026-00582	3.5	More Details
CVE-2026-45781	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.9, OCI ownership validation skips label-match check when upstream OCI registry returns HTTP 429, letting any authenticated publisher bind their io.github.<user>/* namespace to OCI images they do not control. internal/validators/registries/oci.go:104-119 fails open on http.StatusTooManyRequests: when the registry's anonymous fetch to the upstream OCI registry is rate-limited, ValidateOCI returns nil and the publish is accepted without ever running the io.modelcontextprotocol.server.name label-match check at lines 122-141. That label check is the only cross-system ownership proof the registry applies to OCI packages — every other registry type (NPM, PyPI, NuGet, MCPB) treats a non-200 upstream response as a hard error. This vulnerability is fixed in 1.7.9.	3.5	More Details
CVE-2026-8770	A vulnerability was identified in continuedev continue up to 1.2.22. This affects the function lsTool of the file core/tools/implementations/lsTool.ts of the component JSON-RPC Server. Such manipulation of the argument dirPath leads to path traversal. An attack has to be approached locally. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2026-47091	Claude HUD through 0.0.12, patched in commit 234d9aa, contains a path traversal vulnerability that allows attackers to read arbitrary files by supplying an unvalidated transcript_path value via stdin JSON. Attackers can access any file readable by the process and the file metadata is written to a persistent cache file with insufficient permissions, creating a forensic record of accessed paths that survives process exit.	3.3	More Details
CVE-2026-27781	in OpenHarmony v6.0 and prior versions allow a local attacker cause DOS.	3.3	More Details
CVE-2026-28751	in OpenHarmony v6.0 and prior versions allow a local attacker cause DOS.	3.3	More Details
CVE-2026-33565	in OpenHarmony v6.0 and prior versions allow a local attacker cause DOS.	3.3	More Details
CVE-2026-25110	in OpenHarmony v6.0 and prior versions allow a local attacker cause DOS.	3.3	More Details
CVE-2026-4053	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to enforce the PostEditTimeLimit on non-message post fields which allows an authenticated user to modify post file attachments, props, and pin status after the edit window has expired via the post patch and update API endpoints.. Mattermost Advisory ID: MMSA-2026-00631	3.1	More Details
CVE-2026-6334	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to enforce client identity binding during the OAuth authorization code redemption flow which allows an authenticated OAuth client to redeem authorization codes issued to a different client via a crafted token exchange request.. Mattermost Advisory ID: MMSA-2026-00570	3.1	More Details
CVE-2026-8556	Inappropriate implementation in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-8545	Object corruption in Compositing in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-8741	A vulnerability has been found in EMQX up to 6.2.0. This affects an unknown function of the file apps/emqx/src/emqx_persistent_session_ds.erl of the component QoS 2 PUBLISH Packet Handler. Such manipulation leads to race condition. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is reported as difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	3.1	More Details
CVE-2026-8579	Insufficient validation of untrusted input in Skia in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted print file. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-4286	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to check if {{team_id}} was being changed when updating playbooks, allowing users with only {{Manage Playbook Configurations}} permission to change a playbook's team, bypassing manage members restriction via PUT api. Mattermost Advisory ID: MMSA-2025-00552	3.1	More Details
CVE-2026-8553	Use after free in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-8536	Insufficient validation of untrusted input in ReadingMode in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass site Isolation via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-8554	Type Confusion in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-8568	Insufficient policy enforcement in AI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass Site Isolation via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-8572	Insufficient policy enforcement in Network in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details

CVE-2026-8578	Out of bounds read in GPU in Google Chrome on Linux prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-27680	Due to improper input handling under certain conditions, SAP NetWeaver Application Server ABAP allows an attacker to inject custom Cascading Style Sheets (CSS) data into a web page served by the application. When a user accesses or clicks the affected page, the injected CSS is executed. As a result, the issue has a low impact on confidentiality, while integrity and availability are not impacted.	3.1	More Details
CVE-2025-62312	HCL AION is affected by a vulnerability where basic authorization tokens are used for authentication. Use of basic authorization mechanisms may expose credentials to potential interception or misuse, especially if not combined with secure transmission practices.	3.0	More Details
CVE-2026-41963	Stack overflow vulnerability in the media platform. Impact: Successful exploitation of this vulnerability may affect availability.	2.8	More Details
CVE-2026-8200	When schema validation is enabled on a collection and an update or insert would violate the collection's schema, the local server log message generated may not have all user data redacted. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2.7	More Details
CVE-2026-2900	GitLab has remediated an issue in GitLab EE affecting all versions from 16.10 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that when instance-level approval rule editing prevention was enabled, could have allowed an authenticated user with Maintainer permissions to modify or delete project approval rules due to missing authorization checks.	2.7	More Details
CVE-2026-6883	GitLab has remediated an issue in GitLab EE affecting all versions from 15.7 before 18.9.7, 18.10 before 18.10.6, and 18.11 before 18.11.3 that could have allowed an authenticated user to bypass merge request approval requirements due to improper cleanup of orphaned policy records.	2.6	More Details
CVE-2025-62317	HCL AION is affected by a vulnerability where sensitive information may be included in URL parameters. Passing sensitive data in URLs may expose it through browser history, logs, or intermediary systems, potentially leading to unintended information disclosure under certain conditions.	2.6	More Details
CVE-2025-62309	HCL AION is affected by a vulnerability where auto-complete functionality is enabled for certain input fields. This may allow sensitive information to be stored in the browser, potentially leading to unintended exposure under specific conditions.	2.6	More Details
CVE-2026-44638	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. From to 1.8.7-r1, a wrong NULL check after an allocation call in sixel_decode_raw and sixel_decode causes a NULL pointer dereference whenever the allocation fails. The check tests the address of the output parameter (always non-NULL) instead of the value the malloc returned. On allocation failure, the function continues and writes through a NULL pointer, crashing the process. This is a denial of service against any caller of these public APIs that hits a low-memory condition. This vulnerability is fixed in 1.8.7-r2.	2.5	More Details
CVE-2026-44348	PoDoFo is a C++17 PDF manipulation library. From 1.0.0 to before 1.0.4, a double-free vulnerability exists in compute_hash_to_sign() in src/podofo/private/OpenSSLInternal_Ripped.cpp. If EVP_DigestFinal fails after buf has already been freed, the Error label frees buf a second time, causing heap corruption. This vulnerability is fixed in 1.0.4.	2.5	More Details
CVE-2025-62316	HCL AION is affected by a vulnerability where certain security-related HTTP response headers are not properly configured. Absence of these headers may reduce the effectiveness of browser-based security controls and could expose the application to limited security risks under specific conditions.	2.3	More Details
CVE-2026-30904	Protection Mechanism Failure in Zoom Workplace for iOS before version 7.0.0 may allow an authenticated user to conduct a disclosure of information via physical access.	1.8	More Details
CVE-2026-44283	etcd is a distributed key-value store for the data of a distributed system. Prior to 3.4.44, 3.5.30, and 3.6.11, a vulnerability in etcd allows read access via PrevKv, or lease attachment in Put requests within transaction operations, to bypass RBAC authorization checks. An authenticated user without sufficient read or lease-related permissions may be able to access unauthorized data or attach leases by invoking transaction operations with these features enabled. This vulnerability is fixed in 3.4.44, 3.5.30, and 3.6.11.	0.0	More Details
CVE-2026-33637	Faraday is an HTTP client library abstraction layer that provides a common interface over many adapters. Versions 2.0.0 through 2.14.1 still allow protocol-relative host override when the request target is passed as a URI object (rather than a String) to Faraday::Connection#build_exclusive_url. This bypasses the February 2026 fix for GHSA-33mh-2634-fwr2 and enables off-host request forgery: a request built from a fixed-base Faraday::Connection can be redirected to an attacker-controlled host, forwarding connection-scoped values such as Authorization headers and default query parameters. This issue has been fixed in version 2.14.3.	0.0	More Details
CVE-2026-8491	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal Node View Permissions allows Forceful Browsing. This issue affects Node View Permissions: from 0.0.0 before 1.7.0, from 2.0.0 before 2.0.1.	N/A	More Details
CVE-2026-46724	The file indexer does not normalize the configured directory path. A backend user with permission to edit indexer configurations can index documents from arbitrary locations on the server file system through path traversal sequences.	N/A	More Details
CVE-2026-46723	The additional_tables configuration of the page and tt_content indexers accepts arbitrary table and field names. A backend user with permission to edit indexer configurations can copy sensitive data from internal TYPO3 tables into the search index.	N/A	More Details
CVE-2026-6871	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Obfuscate allows Cross-Site Scripting (XSS). This issue affects Obfuscate: from 0.0.0 before 2.0.2.	N/A	More Details
CVE-2026-34579	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior are vulnerable to Authorization Bypass through the private issue monitoring feature . Using a crafted POST request to bug_monitor_add.php, a user with project-level access can add themselves as a monitor for a private issue they do not have access to. Despite displaying an Access Denied error, the application accepts the request and creates a monitor relationship for the private issue. Direct access to the private issue remains blocked, but the user will receive email notifications for updates, leading to disclosure of the private issue's metadata and content. This issue has been	N/A	More Details

	fixed in version 2.28.2.		
CVE-2026-46722	The OOXML parsing of the file indexer does not disable external entity resolution. A crafted xlsx or pptx document placed in an indexed directory can cause local files to be read or outbound HTTP requests to be performed, with the retrieved content being written to the search index.	N/A	More Details
CVE-2026-46721	The create and edit flows do not restrict which user properties may be submitted and do not enforce access control on the frontend user group assignment. As a result, an attacker can assign an arbitrary frontend user group to a newly registered or edited account, gaining unauthorized access to content and functionality restricted to privileged frontend user groups.	N/A	More Details
CVE-2026-2611	In MLflow version 3.9.0, the MLflow Assistant feature introduced improper origin validation in its /ajax-api endpoints. This vulnerability allows a remote attacker to exploit cross-origin requests from a malicious webpage to interact with the MLflow Assistant running on a victim's local machine. By bypassing the loopback-only restriction, the attacker can modify the Assistant's configuration to enable full access, which in turn allows the execution of arbitrary commands via the Claude Code sub-agent. This issue is resolved in version 3.10.0.	N/A	More Details
CVE-2026-30117	scalar/astro v0.1.13 was discovered to contain an arbitrary file upload vulnerability in the the scalar_url query parameter of the Scalar Proxy endpoint. This vulnerability allows attackers to execute arbitrary code via uploading a crafted SVG file.	N/A	More Details
CVE-2026-30118	scalar/astro v0.1.13 was discovered to contain a Server-Side Request Forgery (SSRF) in the scalar_url query parameter of the Scalar Proxy endpoint. This vulnerability allows unauthenticated attackers to force the backend server to send HTTP requests to attacker-controlled URLs, leading to authentication cookies and headers exposure and possible privilege escalation.	N/A	More Details
CVE-2026-32994	The /api/v1/autotranslate.translateMessage endpoint in versions <8.5.0, <8.4.2, <8.3.4, <8.2.4, <8.1.5, <8.0.6, <7.13.8, and <7.10.12 allows any authenticated user to retrieve the full content of any message from any room (private groups, direct messages, channels) by simply providing the target message ID. The endpoint fetches the message via Messages.findOneById(messageId) with no room access check (canAccessRoomIdAsync is never called), returning the complete IMessage object including message text, sender info, room ID, timestamps, and markdown content.	N/A	More Details
CVE-2026-31069	BillaBear (all versions prior to Jan 2026) contains a SQL Injection vulnerability in the EventRepository. User-controlled input from metric filter names and aggregation properties is directly interpolated into SQL queries using sprintf() without proper sanitization or identifier quoting. Although filter values are parameterized, the filter identifiers (keys) are not. An authenticated attacker with ROLE_ACCOUNT_MANAGER permissions can exploit this to execute arbitrary SQL commands.	N/A	More Details
CVE-2026-31070	The LalanaChami Pharmacy Management System (commit 5c3d028) allows unauthenticated remote attackers to escalate privileges by self-assigning an administrative role during registration. The /api/user/signup endpoint fails to validate the role parameter in the request body	N/A	More Details
CVE-2026-31071	API endpoints in LalanaChami Pharmacy Management System (commit 5c3d028) lack authentication middleware. Unauthenticated remote attackers can exploit this to dump all user records (including bcrypt password hashes) via /api/user/getUserData, modify drug inventory, and access private medical prescription data via /api/doctorOder.	N/A	More Details
CVE-2026-31072	The JSONSerializer and CBORSerializer in APScheduler (all versions including 3.10.x and 4.0.0a5) are vulnerable to Remote Code Execution (RCE) via Insecure Deserialization. The unmarshal_object function allows for arbitrary class instantiation and state injection by dynamically importing modules and calling __setstate__ on any class available in the Python environment. An attacker can exploit this by submitting a specially crafted JSON or CBOR payload to an application using these serializers	N/A	More Details
CVE-2026-34154	Discourse is an open-source discussion platform. In versions prior to 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1, a vulnerability in the discourse-subscriptions plugin allows users to gain access to subscription-gated groups without completing payment. This issue has been fixed in versions 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1.	N/A	More Details
CVE-2026-37281	An OS command injection vulnerability in the /stream-to-vlc Express route in hitarth-gg Zenshin before 2.7.0 allows remote attackers to execute arbitrary commands via the url parameter.	N/A	More Details
CVE-2026-8603	In ScadaBR version 1.2.0, an OS Command Injection vulnerability could allow an attacker to execute commands as root on the SCADA system.	N/A	More Details
CVE-2026-39250	An authorization vulnerability exists in Innoshop 0.6.0. After logging into the frontend, an attacker can directly access backend application interfaces, leading to further dangerous operations.	N/A	More Details
CVE-2026-5090	Template::Plugin::HTML versions through 3.102 for Perl allows HTML and JavaScript to be injected. The html_filter function did not escape single quotes. HTML attributes inside of single quotes could be have code injected. For example, the variable "var" in <a id='ref' title='[% var | html %]'> would not be properly escaped. An attacker could insert some limited HTML and JavaScript, for example, var = " ' onclick='while (true) { alert(1) }'" Note that arbitrary HTML and JavaScript would be difficult to inject, because angle brackets, ampersands and double-quotes would still be escaped.	N/A	More Details
CVE-2026-8602	In ScadaBR version 1.2.0, a Missing Authentication for Critical Function vulnerability could allow an unauthenticated attacker to send a HTTP GET requests to the SCADA system and inject arbitrary sensor readings.	N/A	More Details
CVE-2026-5511	In the web management interface of Archer AX72 (SG) v1, the network diagnostic feature improperly handles invalid user input, resulting in limited exposure of diagnostic command usage information. An authenticated attacker with administrative privileges could exploit this issue to confirm the presence of the diagnostic utility and view its valid command-line syntax and options. The exposed information is limited in scope and does not include sensitive system data.	N/A	More Details
CVE-2024-36343	Improper input validation in the System Management Mode (SMM) communications buffer could allow a privileged attacker to perform an out of bounds read or write to a limited section of the Top of Memory Segment (TSEG) memory region, potentially resulting in loss of confidentiality or integrity.	N/A	More Details
CVE-2026-33514	Discourse is an open-source discussion platform. In versions prior to 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1, an authenticated user on a Discourse instance with the form templates feature enabled can read the name and structured content of form templates that are intended exclusively for categories they are not authorized to access. Impact is limited to disclosure of site	N/A	More Details

	configuration metadata. This issue has been fixed in versions 2026.1.4, 2026.3.1, 2026.4.1 and 2026.5.0-latest.1.		
CVE-2026-34390	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior have a Privilege Escalation vulnerability where insufficient access control checks in ProjectUsersAddCommand (manage_proj_user_add.php) allow users having manage_project_threshold access level (manager by default) to grant project-level administrator access to any user (including themselves) in any Project they have manager rights in. The normal project-user add form restricts the selectable access levels to the actor's own project role or below. However, the backend handler still accepts a forged higher access_level value and writes it. The consequences of the privilege escalation are slight, as having administrator access at Project level is effectively not very different from being manager, and it does not actually give administrator privileges on the whole MantisBT instance. In particular, it does not let the upgraded user delete the Project or grant them any access to global administrative functions such as managing Users, Projects, Plugins, Custom Fields, etc. This issue has been fixed in version 2.28.2.	N/A	More Details
CVE-2026-8492	Modification of Assumed-Immutable Data (MAID) vulnerability in Drupal Translate Drupal with GTranslate allows Resource Location Spoofing. This issue affects Translate Drupal with GTranslate: from 0.0.0 before 3.0.5.	N/A	More Details
CVE-2026-8493	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Colorbox Inline allows Cross-Site Scripting (XSS). This issue affects Colorbox Inline: from 0.0.0 before 2.1.1.	N/A	More Details
CVE-2026-34463	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior contain a Stored XSS vulnerability. When cloning an issue originating from a Project other than the current one, the clone form (bug_report_page.php) prepends the source Project name before the category selector without proper escaping, allowing an attacker able to to inject HTML if they can set the Project's name (which typically requires manager or administrator access level). This issue has been resolved in version 2.28.2.	N/A	More Details
CVE-2026-6009	Java Deserialisation Vulnerability in Jaspersoft Reports Library leads to Remote Code Execution (RCE), potentially allowing code execution on the affected system	N/A	More Details
CVE-2026-8967	Information disclosure in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	N/A	More Details
CVE-2026-8966	Information disclosure in the IP Protection component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	N/A	More Details
CVE-2026-46725	The extension passes an attacker-controlled cookie directly to PHP's unserialize() without safely processing the input. A remote, unauthenticated attacker can supply a crafted serialized payload to trigger PHP Object Injection, leading to Remote Code Execution on the TYPO3 server. Exploitation requires the content element to be configured with "Persistent Mode: Static" in the plugin settings.	N/A	More Details
CVE-2026-8604	In ScadaBR version 1.2.0, a CSRF vulnerability could allow an attacker to trigger any authenticated action through a victim's session by luring any logged-in user to a malicious webpage.	N/A	More Details
CVE-2026-6354	Rejected reason: Voluntarily withdrawn	N/A	More Details
CVE-2026-47323	Camel-CXF and Camel-Knative Message Header Injection via Missing Inbound Filtering The CXF and Knative HeaderFilterStrategy implementations (CxfRsHeaderFilterStrategy in camel-cxf-rest, CxfHeaderFilterStrategy in camel-cxf-transport, and KnativeHttpHeaderFilterStrategy in camel-knative-http) only filter outbound Camel-internal headers via setOutFilterStartsWith, while not configuring inbound filtering via setInFilterStartsWith. As a result, an unauthenticated attacker can inject Camel-internal headers (e.g. CamelExecCommandExecutable, CamelFileName) via HTTP requests to CXF-RS or CXF-SOAP endpoints. When a route forwards messages from these endpoints to header-driven components such as camel-exec or camel-file, the injected headers override configured values, enabling remote code execution or arbitrary file writes. This is the same pattern that was previously addressed in camel-undertow (CVE-2025-30177), the broader incoming-header filter (CVE-2025-27636 and CVE-2025-29891), and non-HTTP strategies (CVE-2026-40453). This issue affects Apache Camel: from 3.18.0 before 4.14.6, from 4.15.0 before 4.18.2. Users are recommended to upgrade to version 4.19.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.2. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6.	N/A	More Details
CVE-2026-42100	Improper Handling of Syntactically Invalid Structure in Sparx Pro Cloud Server allows Denial of Service (DoS) attack to be executed by sending an specially crafted SQL query. This causes the Pro Cloud Server service to terminate unexpectedly. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.1 (build 167) and below were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-42099	Sparx Pro Cloud Server is vulnerable to a Race Condition in the /data_api/dl_internal_artifact.php endpoint. The application downloads the properties of the object pointed by guid parameter and saves loaded content in current location (__DIR__) under the specified name. An attacker with repository access can control both the filename and file contents, allowing the creation of a malicious PHP file in a current directory. Although the file is deleted after processing, a race condition exists: if the response transmission is delayed (e.g., via a large file or slow client connection), the file remains accessible. During this window, the attacker can issue a second request to execute the malicious PHP file, resulting in remote code execution. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.1 (build 167) and below were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-42098	Sparx Enterprise Architect software has a security feature that limits user's actions to those specified in the role. An authenticated attacker can modify the Enterprise Architect client behavior (e.g. using a debugger) and log in as any other user or administrator - then it is possible to do every possible change to the repository. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 17.1 and below were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-42097	Sparx Pro Cloud Server requires authentication based on requested URL. An attacker can omit the "model" query parameter and send the model name only in the binary blob in POST request allowing SQL query execution without authentication. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.1 (build 167) and below were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details

CVE-2026-8370	Execution with unnecessary privileges vulnerability in Broadcom Automic Automation Agent Unix on Linux x64, Linux Power 64 BE, Linux Power 64 LE, zLinux (zSeries), AIX, Solaris x64, Solaris Sparc 64 allows Privilege Escalation, Target Programs with Elevated Privileges. This issue affects Automic Automation: < 24.4.4 HF1.	N/A	More Details
CVE-2026-42096	Sparx Pro Cloud Server is vulnerable to Broken Access Control within communication with the database. Due to lack of permission checks, any low privileged user can run arbitrary SQL queries within database user context. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.1 (build 167) and below were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-14575	An Uncontrolled Search Path Element vulnerability in the OpenSSL TLS backend of Qt Network (qtbase) in Qt Qt Framework (Unix) allows a local attacker to load a rogue CA certificate as a trusted system authority via a crafted certificate file placed in the application's working directory.	N/A	More Details
CVE-2026-7860	A possible information disclosure vulnerability exists in the Vaadin Maven plugin and Vaadin Gradle plugin that exposes the full set of environment variables in build logs whenever the frontend build process exits with a non-zero status. Because the build environment may contain credentials supplied as secrets, any failed frontend build can expose those secrets in clear text in CI logs and archived build artifacts. Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include: Product version Vaadin 23.0.0 - 23.6.9 Vaadin 24.0.0 - 24.10.3 Vaadin 25.0.0 - 25.1.4 Mitigation Upgrade to 23.6.10 Upgrade to 24.10.4 or newer Upgrade to 25.1.5 or newer Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 23, 24, or 25 version. ArtifactsMaven coordinatesVulnerable versionsFixed versioncom.vaadin:flow-plugin-base23.0.0 - 23.6.10≥23.6.11com.vaadin:flow-plugin-base24.0.0 - 24.10.3≥24.10.4com.vaadin:flow-plugin-base25.0.0 - 25.1.4≥25.1.5com.vaadin:flow-maven-plugin23.0.0 - 23.6.10≥23.6.11com.vaadin:flow-maven-plugin24.0.0 - 24.10.3≥24.10.4com.vaadin:flow-maven-plugin25.0.0 - 25.1.4≥25.1.5com.vaadin:flow-gradle-plugin24.0.0 - 24.10.3≥24.10.4com.vaadin:flow-gradle-plugin25.0.0 - 25.1.4≥25.1.5	N/A	More Details
CVE-2026-33052	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.0 and 2.28.1 allow a low-privileged authenticated user assigned the "add_profile_threshold" permission to create a global profile despite not having manage_global_profile_threshold, by tampering with the user_id parameter in a valid profile creation request. This issue has been fixed in version 2.28.2.	N/A	More Details
CVE-2026-6367	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core: from 11.3.0 before 11.3.7.	N/A	More Details
CVE-2026-6366	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core: from 8.0.0 before 10.5.9, from 10.6.0 before 10.6.7, from 11.0.0 before 11.2.11, from 11.3.0 before 11.3.7.	N/A	More Details
CVE-2026-6365	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core: from 8.0.0 before 10.5.9, from 10.6.0 before 10.6.7, from 11.0.0 before 11.2.11, from 11.3.0 before 11.3.7.	N/A	More Details
CVE-2026-6095	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Orejime allows Cross-Site Scripting (XSS). This issue affects Orejime: from 0.0.0 before 2.0.16.	N/A	More Details
CVE-2026-34744	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.28.1 and prior permit a user to list and download their own attachments from an Issue created by another user even after it becomes private, bypassing read access revocation. The loss of confidentiality caused by this vulnerability is minimal, considering that only attachments previously uploaded by the user themselves remain accessible. This issue has been fixed in version 2.82.2.	N/A	More Details
CVE-2026-43493	In the Linux kernel, the following vulnerability has been resolved: crypto: pcrypt - Fix handling of MAY_BACKLOG requests MAY_BACKLOG requests can return EBUSY. Handle them by checking for that value and filtering out EINPROGRESS notifications.	N/A	More Details
CVE-2026-43492	In the Linux kernel, the following vulnerability has been resolved: lib/crypto: mpi: Fix integer underflow in mpi_read_raw_from_sgl() Yiming reports an integer underflow in mpi_read_raw_from_sgl() when subtracting "lzeros" from the unsigned "nbytes". For this to happen, the scatterlist "sgl" needs to occupy more bytes than the "nbytes" parameter and the first "nbytes + 1" bytes of the scatterlist must be zero. Under these conditions, the while loop iterating over the scatterlist will count more zeroes than "nbytes", subtract the number of zeroes from "nbytes" and cause the underflow. When commit 2d4d1eea540b ("lib/mpi: Add mpi sgl helpers") originally introduced the bug, it couldn't be triggered because all callers of mpi_read_raw_from_sgl() passed a scatterlist whose length was equal to "nbytes". However since commit 63ba4d67594a ("KEYS: asymmetric: Use new crypto interface without scatterlists"), the underflow can now actually be triggered. When invoking a KEYCTL_PKEY_ENCRYPT system call with a larger "out_len" than "in_len" and filling the "in" buffer with zeroes, crypto_akcipher_sync_prep() will create an all-zero scatterlist used for both the "src" and "dst" member of struct akcipher_request and thereby fulfil the conditions to trigger the bug: sys_keyctl() keyctl_pkey_e_d_s() asymmetric_key_eds_op() software_key_eds_op() crypto_akcipher_sync_encrypt() crypto_akcipher_sync_prep() crypto_akcipher_encrypt() rsa_enc() mpi_read_raw_from_sgl() To the user this will be visible as a DoS as the kernel spins forever, causing soft lockup splats as a side effect. Fix it.	N/A	More Details
CVE-2026-32312	GLPI is a free asset and IT management software package. In versions 11.0.0 through 11.0.6, an authenticated user with forms READ permission can export the structure of unauthorized forms. This issue has been fixed in version 11.0.7.	N/A	More Details
CVE-2026-43491	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: ns: Limit the maximum server registration per node Current code does no bound checking on the number of servers added per node. A malicious client can flood NEW_SERVER messages and exhaust memory. Fix this issue by limiting the maximum number of server registrations to 256 per node. If the NEW_SERVER message is received for an old port, then don't restrict it as it will get replaced. While at it, also rate limit the error messages in the failure path of qrtr_ns_worker(). Note that the limit of 256 is chosen based on the current platform requirements. If requirement changes in the future, this limit can be increased.	N/A	More Details
CVE-2026-8827	The AddressRepository::getSqlQuery() method constructs a database query without properly sanitizing user input, leading to SQL Injection. The method is not invoked anywhere within the extension itself and therefore poses no direct risk in a default installation. However, custom extensions that call this method with untrusted input would expose the site to SQL injection.	N/A	More Details
CVE-2026-8727	The Crawler extension passes the X-T3Crawler-Meta response header from crawled URLs directly to PHP's unserialize(). An attacker controlling a crawled endpoint can inject arbitrary serialized PHP objects, leading to Remote Code Execution on the TYPO3 server. Exploitation requires administrative privileges to configure a crawler-enabled page and trigger the crawl via a Scheduler task.	N/A	More Details

CVE-2026-8605	In ScadaBR version 1.2.0, a Use of Hard-Coded Credentials vulnerability could allow an attacker to access the SCADA system as admin.	N/A	More Details
CVE-2026-8961	Spoofing issue in the Form Autofill component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	N/A	More Details
CVE-2026-8962	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	N/A	More Details
CVE-2026-8726	The extension fails to properly sanitize user input before using it in a database query. As a result, an unauthenticated attacker can inject arbitrary SQL through a URL parameter on pages using the "Date Menu of news articles" plugin. Exploitation requires the "Date Menu of news articles" plugin to be in use and the TypoScript/Plugin setting disableOverrideDemand not to be enabled.	N/A	More Details
CVE-2026-8965	Information disclosure in the DOM: Security component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	N/A	More Details
CVE-2024-36315	Improper enforcement of the LFENCE serialization property may allow an attacker to bypass speculation barriers and potentially disclose sensitive information, potentially resulting in loss of confidentiality.	N/A	More Details
CVE-2026-44647	OneDev is a Git server with CI/CD, kanban, and packages. Prior to 15.0.2, there is behavior that breaks the expected boundary between repository-controlled LFS metadata and server-local filesystem paths. A repository object can steer raw blob reads to arbitrary local files that the server account can access. User with push permission to any repository will be able to access any server files accessible by server process. This vulnerability is fixed in 15.0.2.	N/A	More Details
CVE-2026-4137	In mlflow/mlflow versions prior to 3.11.0, the `get_or_create_nfs_tmp_dir()` function in `mlflow/utils/file_utils.py` creates temporary directories with world-writable permissions (0o777), and the `_create_model_downloading_tmp_dir()` function in `mlflow/pyfunc/__init__.py` creates directories with group-writable permissions (0o770). These insecure permissions allow local attackers to tamper with model artifacts, such as cloudpickle-serialized Python objects, and achieve arbitrary code execution when the tampered artifacts are deserialized via `cloudpickle.load()`. This vulnerability is particularly critical in environments with shared NFS mounts, such as Databricks, where NFS is enabled by default. The issue is a continuation of the vulnerability class addressed in CVE-2025-10279, which was only partially fixed.	N/A	More Details
CVE-2026-0249	Multiple improper certificate validation vulnerabilities in the Palo Alto Networks GlobalProtect™ app enables an attacker to intercept encrypted communications and potentially compromise the endpoint. This can enable a local non-administrative operating system user or an attacker on the same subnet to redirect traffic to an unauthorized server and facilitate the installation of malicious software. The GlobalProtect app on Linux, Windows, iOS and GlobalProtect UWP app are not affected.	N/A	More Details
CVE-2026-41410	Rejected reason: REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-40520. Reason: This candidate is a duplicate of CVE-2026-40520. Notes: All CVE users should reference CVE-2026-40520 instead of this candidate.	N/A	More Details
CVE-2026-0262	Multiple denial of service vulnerabilities in Palo Alto Networks PAN-OS® software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition by sending specially crafted network traffic. Panorama and Cloud NGFW are not impacted by these vulnerabilities.	N/A	More Details
CVE-2026-0261	Multiple command injection vulnerabilities in Palo Alto Networks PAN-OS® software enable an authenticated administrator to bypass system restrictions and run arbitrary commands as a root user. To be able to exploit this issue, the user must have access to the PAN-OS CLI or Web UI. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators and by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma Access® are not impacted by these vulnerabilities.	N/A	More Details
CVE-2026-0259	An arbitrary File Read and Delete Vulnerability in Palo Alto Networks WildFire® WF-500 and WF-500-B appliances enables users to read sensitive information and delete arbitrary files. This vulnerability affects WF-500 and WF-500-B appliances running in the default non-FIPS configuration mode. The WildFire Appliance (WF-500, WF-500-B) software update is now available to customers that use the WildFire Appliance (WF-500, WF-500-B) for on-premise sandboxing. Please note that customers using the WildFire Public cloud service are NOT impacted by this vulnerability.	N/A	More Details
CVE-2026-0258	A server-side request forgery (SSRF) vulnerability in the IKEv2 implementation of Palo Alto Networks PAN-OS® software allows an unauthenticated attacker to cause the firewall to send network requests to unintended destinations or cause a denial of service (DoS) condition. Panorama, Cloud NGFW and Prisma® Access are not impacted by these vulnerabilities.	N/A	More Details
CVE-2026-0257	Authentication bypass vulnerabilities in the GlobalProtect portal and gateway of Palo Alto Networks PAN-OS® software allows the attacker to bypass security restrictions and establish an unauthorized VPN connection. Panorama and Cloud NGFW are not impacted by these issues.	N/A	More Details
CVE-2026-0256	A stored cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS® software enables a malicious authenticated administrator to store a JavaScript payload using the web interface. This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not impacted by this vulnerability.	N/A	More Details
CVE-2026-0251	Multiple local privilege escalation vulnerabilities in the Palo Alto Networks GlobalProtect™ app allow a local user to escalate their privileges to NT AUTHORITY\SYSTEM on Windows and root on macOS and Linux. This enables a non-administrative user to execute arbitrary commands with administrative privileges. The GlobalProtect app on iOS, Android, Chrome OS and GlobalProtect UWP app are not affected.	N/A	More Details
CVE-2026-0250	A buffer overflow vulnerability exists in the Palo Alto Networks GlobalProtect™ app that enables a man in the middle attacker to disrupt system processes and potentially execute arbitrary code with SYSTEM privileges. This vulnerability is triggered during the processing of requests and responses exchanged between Portal and Gateway. The GlobalProtect app on iOS is not affected.	N/A	More Details
CVE-	An improper certificate validation vulnerability in the Prisma Access Agent® for Android and Chrome OS enables an attacker to perform a man-in-the-middle (MitM) attack to intercept VPN traffic. By presenting a certificate for any domain issued by a trusted Certificate		More

2026-0248	Authority, the attacker can capture sensitive device information. The Prisma Access Agent on macOS, Windows, Linux and iOS are not affected.	N/A	Details
CVE-2026-8466	Allocation of Resources Without Limits or Throttling vulnerability in ninenines cowboy allows denial of service via unbounded buffer accumulation in multipart header parsing. cowboy_req:read_part/3 in src/cowboy_req.erl accumulates incoming request bytes into a Buffer binary with no upper-bound check. When cow_multipart:parse_headers/2 returns more or {more, Buffer2}, the function reads up to Length bytes (default 64 KB) from the request body and recurses with the enlarged buffer. There is no equivalent of the byte_size(Acc) > Length guard present in the sibling function read_part_body/4. An unauthenticated attacker can send a multipart/form-data request whose body never yields a complete header section — for example, a body that never contains the advertised boundary delimiter, or one whose header lines never contain \r\n\r\n — and force the server process to accumulate memory linearly with the bytes the protocol layer is willing to deliver. A handful of concurrent such uploads is sufficient to exhaust BEAM memory. This issue affects cowboy from 2.0.0 before 2.15.0.	N/A	More Details
CVE-2026-0247	Multiple authorization bypass vulnerabilities in the Endpoint DLP component of Prisma Access Agent® allow a local attacker to bypass authentication controls and execute privileged operations.	N/A	More Details
CVE-2026-0246	A vulnerability with a privilege management mechanism in the Palo Alto Networks Prisma Access Agent® enables a locally authenticated non-administrative user to escalate their privileges to root on macOS and Linux or NT AUTHORITY\SYSTEM on Windows. This allows the user to execute arbitrary code and read sensitive information otherwise accessible only to privileged accounts. The Prisma Access Agent on iOS, Android and Chrome OS are not affected.	N/A	More Details
CVE-2026-0245	Multiple information disclosure vulnerabilities in Prisma Access Agent® allow a local user to access sensitive configuration data and credentials. The Prisma Access Agent on Linux, ChromeOS, Android, and iOS are not affected.	N/A	More Details
CVE-2026-0244	An improper certificate validation vulnerability in the Palo Alto Networks Prisma SD-WAN ION enables man-in-the-middle (MitM) attacker to impersonate the controller.	N/A	More Details
CVE-2026-0242	A SQL injection vulnerability in Trust Protection Foundation allows an authenticated attacker to execute arbitrary SQL commands against the product database. Successful exploitation could allow an attacker to read sensitive data, modify database contents, and escalate privileges to gain full administrative control of the platform.	N/A	More Details
CVE-2026-0241	Incorrect Authorization vulnerabilities in Trust Protection Foundation allow attackers to bypass access controls and perform unauthorized actions on restricted resources.	N/A	More Details
CVE-2026-0240	An information disclosure vulnerability in Trust Protection Foundation enables an authenticated attacker to obtain sensitive information from the server's vault. Successful exploitation of this issue allows the attacker to impersonate any user within the environment and arbitrarily modify configuration settings.	N/A	More Details
CVE-2026-0239	An information disclosure vulnerability in the Chronosphere Chronocollector enables an unauthenticated attacker with network access to the collector service to retrieve sensitive information.	N/A	More Details
CVE-2026-0238	A vulnerability in Palo Alto Networks Broker VM allows an authenticated administrator to inject arbitrary content into certain Broker VM fields.	N/A	More Details
CVE-2026-43970	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in ninenines cowlib allows unauthenticated remote denial of service via memory exhaustion. cow_spdy:inflate/2 in cowlib passes peer-supplied compressed bytes directly to zlib:inflate/2 with no output size bound. The SPDY header compression dictionary (?ZDICT) is public, and zlib compresses long runs of repeated bytes at roughly 1024:1, so a few kilobytes of SPDY frame payload can decompress to gigabytes on the BEAM heap, OOM-killing the node. A single unauthenticated SPDY frame is sufficient to trigger the condition. The parsers for syn_stream, syn_reply, and headers frame types are all affected via cow_spdy:parse_headers/2. This issue affects cowlib from 0.1.0 before 2.16.1.	N/A	More Details
CVE-2026-0243	A denial of service (DoS) vulnerability in Palo Alto Networks Prisma SD-WAN ION devices enables an unauthenticated attacker in a network adjacent to a Prisma SD-WAN ION device to cause a system disruption by sending a specially crafted IPv6 packet.	N/A	More Details
CVE-2026-26978	FreePBX is an open source IP PBX. In versions below 16.0.71 and 17.0.6, the backup module does not properly sanitize data during restore operations, potentially leading to compromise if the backup contains carefully crafted hostile data. During backup restore operations, FreePBX extracts selected files from a user-supplied tar archive. If a malicious file exists in the archive, it is read and passed directly to unserialize() without validation, class restrictions, or integrity checks. This issue allows Remote Code Execution during restoration of the backup as the web server user (typically asterisk or www-data). The attack does not require shell access, CLI access, or filesystem write permissions beyond the normal restore workflow. Authentication with a known username that has sufficient access permissions and/or write access to backup files is required. This issue has been fixed in versions 16.0.71 and 17.0.6.	N/A	More Details
CVE-2026-44439	PlaywrightCapture is a simple replacement for splash using playwright. Prior to 1.39.6, PlaywrightCapture did not sufficiently restrict navigations and resource requests initiated by rendered pages. An attacker-controlled page could abuse browser-side redirection mechanisms, such as window.location.href, to make the capture process open file:// URLs or request resources hosted on private, loopback, link-local, or otherwise non-public IP addresses. In deployments where PlaywrightCapture processes untrusted URLs, this could allow a remote attacker to perform server-side request forgery against internal services or attempt to access local files from the capture environment. Depending on what capture artifacts are generated and exposed, responses from those resources could potentially be leaked through screenshots, saved page content, logs, or other capture outputs. This vulnerability is fixed in 1.39.6.	N/A	More Details
CVE-2025-62619	Missing authentication in the KVM key download endpoint could allow an unauthenticated attacker with knowledge of the exposed URL to retrieve sensitive keys, potentially leading to loss of confidentiality.	N/A	More Details
CVE-2026-1630	WEBCON BPS is vulnerable to Reflected XSS via one of parameters used by "/openinmobileapp" endpoint. An attacker can send a specially crafted URL that, when opened by an authenticated user, results in arbitrary JavaScript execution in the victim's browser. This issue was fixed in versions 2026.1.3.109 and 2025.2.1.293.	N/A	More Details
	Unsafe object reference (IDOR) in Stel Order v3.25.1 and earlier versions, specifically in the ‘/app/FrontController’ endpoint, through		

CVE-2026-5798	manipulation of the ‘employeeID’ parameter. An authenticated attacker could exploit this vulnerability to access information about any employee (first names, last names, roles, job titles, and vacation records, among others) by modifying that identifier in requests sent to the server.	N/A	More Details
CVE-2026-5790	Stored Cross-Site Scripting (XSS) in Stel Order v3.25.1 and earlier, located at the ‘/app/FrontController’ endpoint via the ‘legalName’ and ‘employeeID’ parameters. The lack of proper input sanitization allows an attacker to inject malicious code that is persistently stored in the database. When other users or administrators access the affected sections, the code executes in their browsers, enabling the theft of session cookies and account hijacking.	N/A	More Details
CVE-2026-8468	Allocation of Resources Without Limits or Throttling vulnerability in plug_project plug allows denial of service via unbounded buffer accumulation in multipart header parsing. 'Elixir.Plug.Conn':read_part_headers/2 in lib/plug/conn.ex does not obey its :length parameter. There is no upper bound on the size of the accumulated buffer. By contrast, the sibling function read_part_body has an explicit byte_size(acc) > length guard that stops accumulation once a limit is reached. No such guard exists in read_part_headers. An unauthenticated remote attacker can exhaust server memory by sending a crafted multipart/form-data request, causing a denial of service. This issue affects plug from 1.4.0 before 1.15.4, 1.16.3, 1.17.1, 1.18.2, and 1.19.2.	N/A	More Details
CVE-2026-8295	An integer overflow vulnerability in the simdjson document-builder API allows incorrect buffer size calculations in "string_builder::escape_and_append()" when processing very large input strings on platforms with limited "size_t" width (e.g., 32-bit builds). The overflow can cause insufficient buffer allocation, leading to out-of-bounds memory reads in SIMD routines and potentially resulting in information disclosure, memory corruption, or malformed JSON output. This vulnerability has been fixed in 4.6.4 release	N/A	More Details
CVE-2025-68421	Comarch ERP Optima client makes use of a hard-coded password for a database user. These credentials cannot be changed. It is possible for a remote attacker to gain an access to the database with elevated privileges including executing system commands on a server. This issue has been fixed in version 2026.4	N/A	More Details
CVE-2025-68420	Comarch ERP Optima client connects to a database using a high privileged account regardless of an application account to which a user logs in. It is possible for a local attacker who controls the client process to dump it's memory, extract credentials and use them to gain a privileged access to the database. In order to exploit this vulnerability, the client application has to be already configured, but a user does not have to be logged in. This issue has been fixed in version 2026.4	N/A	More Details
CVE-2026-41281	Android App "あんしんフィルター for au" provided by KDDI CORPORATION contains Cleartext Transmission of Sensitive Information (CWE-319) vulnerability. A man-in-the-middle attacker may access and modify communications transmitted in plaintext, potentially resulting in information disclosure or data tampering.	N/A	More Details
CVE-2026-44437	The Angular SSR is a server-rise rendering tool for Angular applications. From 19.0.0-next.0 to before 19.2.25, 20.3.25, 21.2.9, and 22.0.0-next.7, a vulnerability exists in the X-Forwarded-Prefix header processing logic within Angular SSR. The internal validation mechanism fails to properly account for URL-encoded characters, specifically dots (%2e%2e). This allows an attacker to bypass security filters by injecting encoded path traversal sequences that are later decoded and utilized by the application logic. When an Angular SSR application is configured to trust proxy headers and is deployed behind a proxy that forwards the X-Forwarded-Prefix header without prior sanitization, an attacker can provide a payload such as /%2e%2e/evil. This vulnerability is fixed in19.2.25, 20.3.25, 21.2.9, and 22.0.0-next.7.	N/A	More Details
CVE-2026-42548	Flight is an extensible micro-framework for PHP. Prior to 3.18.1, Flight::jsonp() concatenates the ?jsonp= query parameter directly into an application/javascript response body without validating that the value is a legal JavaScript identifier. An attacker can inject arbitrary JavaScript that executes in the response origin, enabling reflected cross-site scripting. This vulnerability is fixed in 3.18.1.	N/A	More Details
CVE-2026-44369	CVAT is an open source interactive video and image annotation tool for computer vision. From 2.5.0 to 2.63.0, an attacker who is able to create or edit an annotation guide on a task is able to add malicious JavaScript code, which will then run in the browser of anyone who opens this annotation guide. This code will be able to make arbitrary requests to CVAT with the victim user's privileges. This vulnerability is fixed in 2.64.0.	N/A	More Details
CVE-2026-40328	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-40327	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-8328	The ftpcp() function in Lib/ftplib.py was not updated when CVE-2021-4189 was fixed. While makepasv() was patched to replace server-supplied PASV host addresses with the actual peer address (getpeername()[0]), ftpcp() still calls parse227() directly and passes the raw attacker-controllable IP address and port to target.sendport(). This patch is related to CVE-2021-4189.	N/A	More Details
CVE-2026-44418	EcclesiaCRM is CRM Software for church management. In 8.0.0 and earlier, the ValidateInput() function's default case in EcclesiaCRM's query view passes user-supplied POST parameters directly into SQL queries via str_replace without any sanitization, enabling SQL injection through query parameters that use non-standard validation types. This is caused by an incomplete fix for CVE-2026-35184.	N/A	More Details
CVE-2026-44372	Nitro is a next generation server toolkit. Prior to 3.0.260429-beta, an attacker could turn a redirect route rule using wildcards rewrite into a cross-host redirect by sliding an extra slash in after the rule prefix. This vulnerability is fixed in 3.0.260429-beta.	N/A	More Details
CVE-2026-44368	PyQuorum is a cryptographic library for secret sharing and key management. Prior to 0.2.1, the mul_mod function implements multiplication via a binary expansion loop whose execution time depends on the Hamming weight of the second operand (the exponent). An attacker who can measure the time of secret-sharing operations (e.g., via a remote service) could progressively recover the values of shares, ultimately leading to secret reconstruction. This vulnerability is fixed in 0.2.1.	N/A	More Details
CVE-2026-44364	MISP modules are autonomous modules that can be used to extend MISP for new services. In 3.0.7 and earlier, a Cross-Site Request Forgery vulnerability in the MISP Modules website allowed an attacker to cause an authenticated user to submit unintended requests to the home endpoint. The vulnerability was due to the home blueprint being exempted from CSRF protection. This could allow modification of session query data in the context of the authenticated user. The issue was fixed by enabling CSRF protection for the affected blueprint and hardening query parsing.	N/A	More Details
CVE-	MISP modules are autonomous modules that can be used to extend MISP for new services. Prior to 3.0.7, an unsafe remote resource fetching vulnerability existed in MISP Modules expansion modules. The html_to_markdown module accepted arbitrary HTTP(S) URLs without sufficient validation, which could allow Server-Side Request Forgery against loopback, private, or link-local network resources.		More

2026-44363	Additionally, the qrcode module disabled TLS certificate verification when retrieving remote images, exposing requests to potential man-in-the-middle interception or response tampering. The issue was fixed by validating URL schemes, blocking local and private address ranges, resolving hostnames before fetching, enforcing request timeouts, and re-enabling TLS certificate verification. This vulnerability is fixed in 3.0.7.	N/A	Details
CVE-2026-0236	A code injection vulnerability in Palo Alto Networks Prisma® Browser on macOS fails to properly restrict access to its AppleScript interface allowing a locally authenticated non-admin user to leverage this exposed Apple Event handler to send unauthorized commands to the browser.	N/A	More Details
CVE-2026-0235	A race condition vulnerability in Palo Alto Networks Prisma® Browser enables a locally authenticated non-admin user to bypass certain access and data control policies.	N/A	More Details
CVE-2026-0265	An authentication bypass vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to bypass authentication controls when Cloud Authentication Service (CAS) is enabled. The risk is higher if CAS is enabled on the management interface and lower when any other login interfaces are used. The risk of this issue is greatly reduced if you secure access to the management web interface by restricting access to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma Access® are not impacted by this vulnerability.	N/A	More Details
CVE-2026-25710	The new upstream added a privileged D-Bus helper called plasmaloginauthhelper, which suffers from multiple issues, e.g.aA compromised plasmalogin service account can chown() arbitrary files in the system.	N/A	More Details
CVE-2026-39803	Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of service via memory exhaustion. The chunked clause of 'Elixir.Bandit.HTTP1.Socket':read_data/2 in lib/bandit/http1/socket.ex ignores the caller-supplied :length option when reading HTTP/1 chunked request bodies. Instead of capping the accumulated body at the configured limit (e.g. Plug.Parsers' default 8 MB), do_read_chunked_data!/5 buffers every received chunk into an iolist unconditionally and materializes the entire body as a single binary. The function always returns {:ok, body, ...}, so callers cannot interpose a 413 response. Because Plug.Parsers runs before routing and authentication in the standard Phoenix endpoint, an unauthenticated attacker needs no valid route or credentials. Sending a single Transfer-Encoding: chunked POST request with an arbitrarily large body to any path causes the BEAM process to exhaust available memory and be terminated by the OS OOM killer. The content-length path in the same function correctly enforces the limit and is not affected. This issue affects bandit: from 1.4.0 before 1.11.1.	N/A	More Details
CVE-2026-42961	ELECOM wireless LAN access point devices implement CSRF protection mechanism, but with inadequate handling of CSRF tokens. If a user views a malicious page while logged in, the user may be tricked to do unintended operations.	N/A	More Details
CVE-2026-42950	ELECOM wireless LAN access point devices do not check if language parameter has an appropriate value. If a user views a malicious page while logged in, the admin page on the user's web browser may become broken.	N/A	More Details
CVE-2026-42948	Stored cross-site scripting vulnerability exists in ELECOM wireless LAN access point devices. If one of the administrators input malicious data, an arbitrary script may be executed in another administrative user's web browser.	N/A	More Details
CVE-2026-42062	ELECOM wireless LAN access point devices contain an OS command injection in processing of username parameter. If processing a crafted request, an arbitrary OS command may be executed. No authentication is required.	N/A	More Details
CVE-2026-40621	ELECOM wireless LAN access point devices do not require authentication to access some specific URLs. The affected product may be operated without authentication.	N/A	More Details
CVE-2026-35506	ELECOM wireless LAN access point devices contain an OS command injection vulnerability in processing of ping_ip_addr parameter. If processing a crafted request sent by a logged-in user, an arbitrary OS command may be executed.	N/A	More Details
CVE-2026-25107	ELECOM wireless LAN access point devices use a hard-coded cryptographic key when creating backups of configuration files. An attacker who knows the encryption key can tamper the configuration file of the product, and a victim administrator may be tricked to use a crafted configuration file.	N/A	More Details
CVE-2026-44931	The newly introduced RecordUsage D-Bus method https://gitlab.freedesktop.org/pwithnall/malcontent/-/blob/0.14.0/libmalcontent-timer/child-timer-service.c in malcontent-timerd allows arbitrary users in the system to slowly fill up disk space in /var/lib/malcontent-timerd	N/A	More Details
CVE-2024-47091	Privilege escalation in the mk_mysql agent plugin on Windows in Checkmk <2.4.0p29, <2.3.0p47, and 2.2.0 (EOL) allows a local unprivileged user able to create a Windows service whose name matches 'MySQL' or 'MariaDB' (or with write access to a binary referenced by such a service) to execute arbitrary code in the context of the Checkmk agent service, which typically runs as SYSTEM.	N/A	More Details
CVE-2026-0264	A buffer overflow vulnerability in the DNS proxy and DNS Server features of Palo Alto Networks PAN-OS® Software allows an unauthenticated attacker with network access to cause a denial of service (DoS) condition (all PAN-OS platforms except Cloud NGFW and Prisma Access) or potentially execute arbitrary code by sending specially crafted network traffic (PA-Series hardware only). Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability.	N/A	More Details
CVE-2026-44612	Bytello Share (Windows Edition) installer executable provided by Bytello insecurely loads Dynamic Link Libraries. If there is a crafted DLL at the same directory when invoking the affected installer, arbitrary code may be executed with the privilege of the user invoking the installer.	N/A	More Details
CVE-2026-32661	Stack-based buffer overflow vulnerability exists in GUARDIANWALL MailSuite and GUARDIANWALL Mail Security Cloud (SaaS version). If a remote attacker sends a specially crafted request to the product's web service, arbitrary code may be executed when the product is configured to run pop3wallpasswd with grdnwww user privilege.	N/A	More Details
CVE-2026-	Incorrect authorization in the "submitted together" feature in Gerrit versions 2.12 and later allows an authenticated attacker with force push permissions on a secondary branch to bypass code review and forcefully submit code to restricted branches via a crafted	N/A	More

2725	submission matching the "topic" tag of an unapproved change.		Details
CVE-2026-21024	Improper privilege management in Samsung System Support Service prior to version 8.0.8.0 allows local attackers to trigger privileged functions.	N/A	More Details
CVE-2026-21019	Improper input validation in FacAtFunction in Galaxy Watch prior to SMR May-2026 Release 1 allows local attacker to execute arbitrary code with system privilege.	N/A	More Details
CVE-2025-62627	An untrusted pointer dereference in the ionic cloud driver for VMWare ESXi could allow an attacker with an unprivileged VM to read kernel memory or co-located guest VM memory, potentially resulting in loss of confidentiality or availability.	N/A	More Details
CVE-2025-62624	A heap-based buffer overflow in the ionic cloud driver for VMware ESXi could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2025-62623	A heap-based buffer overflow in the ionic cloud driver for VMware ESXi could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2025-61972	Missing lock bit protection for NBIO registers could allow a local admin-privileged attacker to gain arbitrary System Management Network (SMN) access, potentially resulting in arbitrary code execution in AMD Secure Processor (ASP) and loss of the SEV-SNP guest's confidentiality and integrity.	N/A	More Details
CVE-2026-39806	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in mtrudel bandit allows unauthenticated remote denial of service via worker process exhaustion. 'Elixir.Bandit.HTTP1.Socket':do_read_chunked_data!/5 in lib/bandit/http1/socket.ex terminates only when the last-chunk line 0\r\n is followed immediately by the empty trailer line \r\n. RFC 9112 §7.1.2 permits zero or more trailer fields between them. When trailers are present, none of the match clauses fit: the catch-all arm computes a negative to_read, calls read_available!/2, receives <<>> on timeout, and tail-recurses with unchanged state. The worker process is pinned for the lifetime of the TCP connection. A handful of concurrent connections sending RFC-conformant chunked requests with trailer fields is sufficient to exhaust the Bandit worker pool and render the server unresponsive to all further traffic. No authentication, special headers, or large payload is required. Proxies such as NGINX and HAProxy legitimately forward trailer-bearing requests, so servers behind such proxies may be affected without any malicious client involvement. This issue affects bandit: from 1.6.1 before 1.11.1.	N/A	More Details
CVE-2026-8369	Improper Input Validation in the NAT64 translator in The OpenThread Authors OpenThread before commit 26a882d on all platforms allows an attacker on the adjacent IPv4 network to inject corrupted IPv6 packets into the Thread mesh or bypass security checks via crafted IPv4 packets with options.	N/A	More Details
CVE-2025-32425	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. In AutoGPT, the execution process is recorded to the console (stdout/stderr), and deployed in container mode, which is automatically captured by Docker and stored as "container logs". However, prior to 0.6.32, there is no limit on the log size when the container is deployed. When the number of user accesses is too large, the log on the server disk will be too large, causing disk resource exhaustion and eventually causing DoS. autogpt-platform-beta-v0.6.32 fixes the issue.	N/A	More Details
CVE-2026-42557	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. Prior to 4.5.7, JupyterLab's HTML sanitizer allowlists data-commandlinker-command and data-commandlinker-args on button elements, while CommandLinker listens for all click events on document.body and executes the named command without checking whether the element came from trusted JupyterLab UI. A notebook with a pre-saved HTML cell output containing a deceptive button can trigger arbitrary JupyterLab commands - including arbitrary code execution - on a single user click, without any code being submitted for execution by the user. This vulnerability is fixed in 4.5.7.	N/A	More Details
CVE-2026-0263	A buffer overflow vulnerability in the IKEv2 processing of Palo Alto Networks PAN-OS® software allows an unauthenticated network-based attacker to execute arbitrary code with elevated privileges on the firewall, or cause a denial of service (DoS) condition. Panorama, Cloud NGFW, and Prisma® Access are not impacted by these vulnerabilities.	N/A	More Details
CVE-2026-0237	An improper protection of alternate path vulnerability in Palo Alto Networks Prisma® Browser on macOS fails to properly restrict access to an internal automation bridge. This allows a locally authenticated non-admin user to leverage an exposed communication channel to send unauthorized commands to the browser, bypassing security controls.	N/A	More Details
CVE-2026-45033	GitHub Copilot CLI brings AI-powered coding assistance directly to your command line. Prior to 1.0.43, a security vulnerability has been identified in GitHub Copilot CLI where a malicious bare git repository nested inside a project directory can achieve arbitrary code execution when the agent performs git operations. By exploiting git's automatic bare repository discovery during directory traversal, an attacker can set core.fsmonitor or other executable config keys to run arbitrary commands without user awareness or approval. The vulnerability arises because git's core.fsmonitor config key (and 15+ similar keys such as core.hookspath, diff.external, merge.tool, etc.) can specify arbitrary shell commands that git will execute as part of normal operations like status, diff, or rev-parse. This vulnerability is fixed in 1.0.43.	N/A	More Details
CVE-2026-44470	The Claude Desktop app gives you Claude Code with a graphical interface built for running multiple sessions side by side. Prior to 1.3834.0, the CoworkVMService component in Claude Desktop for Windows ran as SYSTEM and did not validate whether the VM bundle directory was a real directory or an NTFS directory junction before creating files within it. A local non-elevated user could replace the user-writable VM bundle directory with a directory junction pointing to an attacker-chosen location, causing the service to create a SYSTEM-owned file in an arbitrary directory. This could be leveraged for local privilege escalation. This vulnerability is fixed in 1.3834.0.	N/A	More Details
CVE-2026-44467	The Claude Desktop app gives you Claude Code with a graphical interface built for running multiple sessions side by side. From 1.2581.0 to before 1.4304.0, Claude Desktop's SSH remote development feature verified only whether a hostname existed in ~/.ssh/known_hosts without comparing the server's presented host key against the stored key. This allowed a network-positioned attacker to present an arbitrary SSH host key and have the connection silently accepted, enabling a man-in-the-middle attack on remote development sessions. Successful exploitation required the attacker to be in a network position to intercept SSH traffic (e.g., via ARP spoofing, rogue Wi-Fi, or DNS poisoning) and the target hostname to already have an entry in the victim's known_hosts file. This vulnerability is fixed in 1.4304.0.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: liveupdate: luo_file: remember retrieve() status LUO keeps track of successful retrieve attempts on a LUO file. It does so to avoid multiple retrievals of the same file. Multiple retrievals cause problems because once the file is retrieved, the serialized data structures are likely freed and the file is likely in a very different state from what		

CVE-2026-43489	the code expects. The retrieve boolean in struct luo_file keeps track of this, and is passed to the finish callback so it knows what work was already done and what it has left to do. All this works well when retrieve succeeds. When it fails, luo_retrieve_file() returns the error immediately, without ever storing anywhere that a retrieve was attempted or what its error code was. This results in an errored LIVEUPDATE_SESSION_RETRIEVE_FD ioctl to userspace, but nothing prevents it from trying this again. The retry is problematic for much of the same reasons listed above. The file is likely in a very different state than what the retrieve logic normally expects, and it might even have freed some serialization data structures. Attempting to access them or free them again is going to break things. For example, if memfd managed to restore 8 of its 10 folios, but fails on the 9th, a subsequent retrieve attempt will try to call kho_restore_folio() on the first folio again, and that will fail with a warning since it is an invalid operation. Apart from the retry, finish() also breaks. Since on failure the retrieved bool in luo_file is never touched, the finish() call on session close will tell the file handler that retrieve was never attempted, and it will try to access or free the data structures that might not exist, much in the same way as the retry attempt. There is no sane way of attempting the retrieve again. Remember the error retrieve returned and directly return it on a retry. Also pass this status code to finish() so it can make the right decision on the work it needs to do. This is done by changing the bool to an integer. A value of 0 means retrieve was never attempted, a positive value means it succeeded, and a negative value means it failed and the error code is the value.	N/A	More Details
CVE-2026-43488	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Prevent interrupt storm on host controller error (HCE) The xHCI controller reports a Host Controller Error (HCE) in UAS Storage Device plug/unplug scenarios on Android devices. HCE is checked in xhci_irq() function and causes an interrupt storm (since the interrupt isn’t cleared), leading to severe system-level faults. When the xHC controller reports HCE in the interrupt handler, the driver only logs a warning and assumes xHC activity will stop as stated in xHCI specification. An interrupt storm does however continue on some hosts even after HCE, and only ceases after manually disabling xHC interrupt and stopping the controller by calling xhci_halt(). Add xhci_halt() to xhci_irq() function where STS_HCE status is checked, mirroring the existing error handling pattern used for STS_FATAL errors. This only fixes the interrupt storm. Proper HCE recovery requires resetting and re-initializing the xHC.	N/A	More Details
CVE-2026-43487	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Disable LPM on ST1000DM010-2EP102 According to a user report, the ST1000DM010-2EP102 has problems with LPM, causing random system freezes. The drive belongs to the same BarraCuda family as the ST2000DM008-2FR102 which has the same issue.	N/A	More Details
CVE-2026-43486	In the Linux kernel, the following vulnerability has been resolved: arm64: contpte: fix set_access_flags() no-op check for SMMU/ATS faults contpte_ptep_set_access_flags() compared the gathered ptep_get() value against the requested entry to detect no-ops. ptep_get() ORs AF/dirty from all sub-PTEs in the CONT block, so a dirty sibling can make the target appear already-dirty. When the gathered value matches entry, the function returns 0 even though the target sub-PTE still has PTE_RDONLY set in hardware. For a CPU with FEAT_HAFDBS this gathered view is fine, since hardware may set AF/dirty on any sub-PTE and CPU TLB behavior is effectively gathered across the CONT range. But page-table walkers that evaluate each descriptor individually (e.g. a CPU without DBM support, or an SMMU without HTTU, or with HA/HD disabled in CD.TCR) can keep faulting on the unchanged target sub-PTE, causing an infinite fault loop. Gathering can therefore cause false no-ops when only a sibling has been updated: - write faults: target still has PTE_RDONLY (needs PTE_RDONLY cleared) - read faults: target still lacks PTE_AF Fix by checking each sub-PTE against the requested AF/dirty/write state (the same bits consumed by __ptep_set_access_flags()), using raw per-PTE values rather than the gathered ptep_get() view, before returning no-op. Keep using the raw target PTE for the write-bit unfold decision. Per Arm ARM (DDI 0487) D8.7.1 ("The Contiguous bit"), any sub-PTE in a CONT range may become the effective cached translation and software must maintain consistent attributes across the range.	N/A	More Details
CVE-2026-43485	In the Linux kernel, the following vulnerability has been resolved: nouveau/gsp: drop WARN_ON in ACPI probes These WARN_ONs seem to trigger a lot, and we don't seem to have a plan to fix them, so just drop them, as they are most likely harmless.	N/A	More Details
CVE-2026-43484	In the Linux kernel, the following vulnerability has been resolved: mmc: core: Avoid bitfield RMW for claim/retune flags Move claimed and retune control flags out of the bitfield word to avoid unrelated RMW side effects in asynchronous contexts. The host->claimed bit shared a word with retune flags. Writes to claimed in __mmc_claim_host() or retune_now in mmc_mq_queue_rq() can overwrite other bits when concurrent updates happen in other contexts, triggering spurious WARN_ON(!host->claimed). Convert claimed, can_retune, retune_now and retune_paused to bool to remove shared-word coupling.	N/A	More Details
CVE-2026-43483	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Set/clear CR8 write interception when AVIC is (de)activated Explicitly set/clear CR8 write interception when AVIC is (de)activated to fix a bug where KVM leaves the interception enabled after AVIC is activated. E.g. if KVM emulates INIT=>WFS while AVIC is deactivated, CR8 will remain intercepted in perpetuity. On its own, the dangling CR8 intercept is "just" a performance issue, but combined with the TPR sync bug fixed by commit d02e48830e3f ("KVM: SVM: Sync TPR from LAPIC into VMCB::V_TPR even if AVIC is active"), the danging intercept is fatal to Windows guests as the TPR seen by hardware gets wildly out of sync with reality. Note, VMX isn't affected by the bug as TPR_THRESHOLD is explicitly ignored when Virtual Interrupt Delivery is enabled, i.e. when APICv is active in KVM's world. I.e. there's no need to trigger update_cr8_intercept(), this is firmly an SVM implementation flaw/detail. WARN if KVM gets a CR8 write #VMEXIT while AVIC is active, as KVM should never enter the guest with AVIC enabled and CR8 writes intercepted. [Squash fix to avic_deactivate_vmcb. - Paolo]	N/A	More Details
CVE-2026-43482	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Disable preemption between scx_claim_exit() and kicking helper work scx_claim_exit() atomically sets exit_kind, which prevents scx_error() from triggering further error handling. After claiming exit, the caller must kick the helper kthread work which initiates bypass mode and teardown. If the calling task gets preempted between claiming exit and kicking the helper work, and the BPF scheduler fails to schedule it back (since error handling is now disabled), the helper work is never queued, bypass mode never activates, tasks stop being dispatched, and the system wedges. Disable preemption across scx_claim_exit() and the subsequent work kicking in all callers - scx_disable() and scx_vexit(). Add lockdep_assert_preemption_disabled() to scx_claim_exit() to enforce the requirement.	N/A	More Details
CVE-2026-43481	In the Linux kernel, the following vulnerability has been resolved: net-shapers: don't free reply skb after genlmsg_reply() genlmsg_reply() hands the reply skb to netlink, and netlink_unicast() consumes it on all return paths, whether the skb is queued successfully or freed on an error path. net_shaper_nl_get_doit() and net_shaper_nl_cap_get_doit() currently jump to free_msg after genlmsg_reply() fails and call nlmsg_free(msg), which can hit the same skb twice. Return the genlmsg_reply() error directly and keep free_msg only for pre-reply failures.	N/A	More Details
CVE-2026-43480	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp3x-rt5682-max9836: Add missing error check for clock acquisition The acp3x_5682_init() function did not check the return value of clk_get(), which could lead to dereferencing error pointers in rt5682_clk_enable(). Fix this by: 1. Changing clk_get() to the device-managed devm_clk_get(). 2. Adding proper IS_ERR() checks for both clock acquisitions.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: usb: lan78xx: fix WARN in __netif_napi_del_locked on disconnect Remove redundant netif_napi_del() call from disconnect path. A WARN may be triggered in __netif_napi_del_locked() during USB device disconnect: WARNING: CPU: 0 PID: 11 at net/core/dev.c:7417 __netif_napi_del_locked+0x2b4/0x350 This happens because netif_napi_del() is called in the disconnect path while NAPI is still enabled. However, it is not necessary to call netif_napi_del() explicitly, since unregister_netdev() will handle NAPI teardown automatically and safely. Removing the redundant call avoids triggering the		

CVE-2026-43479	warning. Full trace: lan78xx 1-1:1.0 enu1: Failed to read register index 0x000000c4. ret = -ENODEV lan78xx 1-1:1.0 enu1: Failed to set MAC down with error -ENODEV lan78xx 1-1:1.0 enu1: Link is Down lan78xx 1-1:1.0 enu1: Failed to read register index 0x00000120. ret = -ENODEV ------------[cut here]------------ WARNING: CPU: 0 PID: 11 at net/core/dev.c:7417 __netif_napi_del_locked+0x2b4/0x350 Modules linked in: flexcan can_dev fuse CPU: 0 UID: 0 PID: 11 Comm: kworker/0:1 Not tainted 6.16.0-rc2-00624-ge926949dab03 #9 PREEMPT Hardware name: SKOV IMX8MP CPU revC - bd500 (DT) Workqueue: usb_hub_wq hub_event pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __netif_napi_del_locked+0x2b4/0x350 lr : __netif_napi_del_locked+0x7c/0x350 sp : ffffffc085b673c0 x29: ffffffc085b673c0 x28: ffffff800b7f2000 x27: ffffff800b7f20d8 x26: ffffff80110bcf58 x25: ffffff80110bd978 x24: 1ffffff0022179eb x23: ffffff80110bc000 x22: ffffff800b7f5000 x21: ffffff80110bc000 x20: ffffff80110bcf38 x19: ffffff80110bcf28 x18: dfffffc000000000 x17: ffffffc081578940 x16: ffffffc08284cee0 x15: 0000000000000028 x14: 0000000000000006 x13: 0000000000040000 x12: ffffffb0022179e8 x11: 1ffffff0022179e7 x10: ffffffb0022179e7 x9 : dfffffc000000000 x8 : 0000004ffdde8619 x7 : ffffff80110bcf3f x6 : 0000000000000001 x5 : ffffff80110bcf38 x4 : ffffff80110bcf38 x3 : 0000000000000000 x2 : 0000000000000000 x1 : 1ffffff0022179e7 x0 : 0000000000000000 Call trace: __netif_napi_del_locked+0x2b4/0x350 (P) lan78xx_disconnect+0xf4/0x360 usb_unbind_interface+0x158/0x718 device_remove+0x100/0x150 device_release_driver_internal+0x308/0x478 device_release_driver+0x1c/0x30 bus_remove_device+0x1a8/0x368 device_del+0x2e0/0x7b0 usb_disable_device+0x244/0x540 usb_disconnect+0x220/0x758 hub_event+0x105c/0x35e0 process_one_work+0x760/0x17b0 worker_thread+0x768/0xce8 kthread+0x3bc/0x690 ret_from_fork+0x10/0x20 irq event stamp: 211604 hardirqs last enabled at (211603): [<ffffffc0828cc9ec>] _raw_spin_unlock_irqrestore+0x84/0x98 hardirqs last disabled at (211604): [<ffffffc0828a9a84>] el1_dbg+0x24/0x80 softirqs last enabled at (211296): [<ffffffc080095f10>] handle_softirqs+0x820/0xbc8 softirqs last disabled at (210993): [<ffffffc080010288>] __do_softirq+0x18/0x20 ---[end trace 0000000000000000]--- lan78xx 1-1:1.0 enu1: failed to kill vid 0081/0	N/A	More Details
CVE-2026-43478	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: rt1011: Use component to get the dapm context in spk_mode_put The correct helper to use in rt1011_recv_spk_mode_put() to retrieve the DAPM context is snd_soc_component_to_dapm(), from kcontrol we will receive NULL pointer.	N/A	More Details
CVE-2026-43477	In the Linux kernel, the following vulnerability has been resolved: drm/i915/vrr: Configure VRR timings after enabling TRANS_DDI_FUNC_CTL Apparently ICL may hang with an MCE if we write TRANS_VRR_VMAX/FLIPLINE before enabling TRANS_DDI_FUNC_CTL. Personally I was only able to reproduce a hang (on an Dell XPS 7390 2-in-1) with an external display connected via a dock using a dodgy type-C cable that made the link training fail. After the failed link training the machine would hang. TGL seemed immune to the problem for whatever reason. BSpec does tell us to configure VRR after enabling TRANS_DDI_FUNC_CTL as well. The DMC firmware also does the VRR restore in two stages: - first stage seems to be unconditional and includes TRANS_VRR_CTL and a few other VRR registers, among other things - second stage is conditional on the DDI being enabled, and includes TRANS_DDI_FUNC_CTL and TRANS_VRR_VMAX/VMIN/FLIPLINE, among other things So let's reorder the steps to match to avoid the hang, and toss in an extra WARN to make sure we don't screw this up later. BSpec: 22243 (cherry picked from commit 93f3a267c3dd4d811b224bb9e179a10d81456a74)	N/A	More Details
CVE-2026-43476	In the Linux kernel, the following vulnerability has been resolved: iio: chemical: sps30_i2c: fix buffer size in sps30_i2c_read_meas() sizeof(num) evaluates to sizeof(size_t) (8 bytes on 64-bit) instead of the intended __be32 element size (4 bytes). Use sizeof(*meas) to correctly match the buffer element type.	N/A	More Details
CVE-2025-62625	Improper privilege management in the KVM key download component could allow an attacker to swap tokens and download sensitive keys, potentially resulting in unauthorized access to privileged resources and loss of confidentiality.	N/A	More Details
CVE-2025-62628	Unsafe OpenSSL initialization within some AMD optional tools may allow a local user-privileged attacker to inject a malicious DLL, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2026-21730	Verba is affected by a Stored Cross-Site Scripting (XSS) vulnerability within its login logging mechanism. When an unauthenticated remote attacker attempts to log in using an incorrect username and password combination, the supplied username value is recorded in the application logs. Due to lack of input sanitization, an attacker can inject a malicious XSS payload into the username field. This payload will be executed in the context of the administrator’s browser when the admin accesses the web application's log viewer. The vendor was notified early about this vulnerability, but didn't respond to our messages. This issue was fixed in version 10.0.6	N/A	More Details
CVE-2025-66664	Insufficient parameter sanitization in AMD Secure Processor (ASP) TEE SOC Driver could allow an attacker to issue a malformed DRV_SOC_CMD_ID_LOAD_GFX_IP_FW SR-IOV command to cause out-of-bounds read, potentially resulting in SOC Driver memory contents exposure or an exception	N/A	More Details
CVE-2025-54518	Improper isolation of shared resources within the CPU operation cache on Zen 2-based products could allow an attacker to corrupt instructions executed at a different privilege level, potentially resulting in privilege escalation.	N/A	More Details
CVE-2025-52532	A race condition in the MxGPU-Virtualization driver’s ioctl path caused by concurrent unsynchronized access to the global variable amdgv_cmd in an unlocked ioctl handler could be exploited by an attacker to trigger a heap-based buffer overflow, potentially resulting in denial-of-service within the vulnerable system context.	N/A	More Details
CVE-2024-36334	Improper verification of cryptographic signature in the Radeon RGB tool could allow a malicious file placed in the installation directory to be run with elevated privileges potentially leading to arbitrary code execution.	N/A	More Details
CVE-2024-36323	Improper isolation of VCN-JPEG HW register space could allow a malicious Guest Virtual Machine (VM) or a process to perform unauthorized access to the register space of the JPEG cores assigned a victim VM/process, potentially gaining arbitrary read/write access to the victim VM/process data.	N/A	More Details
CVE-2024-21950	An out of bounds read in the remote management firmware could allow a privileged attacker read a limited section of memory outside of established bounds potentially resulting in loss of confidentiality or availability.	N/A	More Details
CVE-2026-7373	Rapid7 Metasploit Pro is vulnerable to a local privilege escalation attack that allows a user to gain SYSTEM level control of a Windows host. When started the metasploitPostgreSQL service would start the postgres.exe child process which would in turn load an OpenSSL configuration file from a static location. This static location would be writable by a pre-existing "vagrant" user, if they already existed on the system. Metasploit does not create local accounts, an Administrator would need to create it. By planting a crafted openssl.cnf file an attacker can trick the high-privilege service into executing arbitrary commands. This effectively permits the unprivileged vagrant user to bypass security controls and achieve a full host compromise under the agent's SYSTEM level access.	N/A	More Details
CVE-	A vulnerability in mlflow/mlflow versions 3.9.0 and earlier allows unauthenticated access to certain FastAPI routes when the server is started with authentication enabled (`--app-name basic-auth`) and served via uvicorn (ASGI). The FastAPI permission middleware only enforces authentication on `/gateway/` routes, leaving other routes such as the Job API (`/ajax-api/3.0/jobs/*`) and the OpenTelemetry		

2026-2652	trace ingestion API (`/v1/traces`) unprotected. This allows unauthenticated remote attackers to submit jobs, read job results, cancel running jobs, and inject arbitrary trace data into experiments. The issue arises from an architectural mismatch between Flask and FastAPI authentication mechanisms, where the `_find_fastapi_validator()` function fails to handle non-`/gateway/` paths, resulting in a complete authentication bypass. This vulnerability is fixed in version 3.10.0.	N/A	More Details
CVE-2026-0428	Insufficient parameter sanitization in TEE SOC Driver could allow an attacker to issue a malformed DRV_SOC_CMD_ID_SRIOV_COPY_VF_CHIPLET_REGS to write invalid data to a remote Die, potentially resulting in unexpected behavior.	N/A	More Details
CVE-2026-0427	Improper cleanup of shared register resources in GPU firmware could allow an admin-privileged attacker from a Guest Virtual machine (VM) to access these shared resources from another Guest VM, potentially resulting in the loss of confidentiality, integrity, or availability.	N/A	More Details
CVE-2025-66660	Insufficient parameter sanitization in TEE SOC Driver could allow an attacker to issue a malformed DRV_SOC_CMD_ID_SRIOV_CHECK_TA_COMPAT to cause incorrect shared memory mapping, potentially resulting in unexpected behavior.	N/A	More Details
CVE-2025-0040	Improper access control between the Joint Test Action Group (JTAG) and Advanced Extensible Interface (AXI) could allow an attacker with physical access to read or overwrite the contents of cross-chip debug (XCD) registers potentially resulting in loss of data integrity or confidentiality.	N/A	More Details
CVE-2025-54517	Out of bounds write in AMD AMDGV_CMD_GET_DIAG_DATA ioctl handler could allow a local user to escalate privileges via remote code execution.	N/A	More Details
CVE-2025-54511	Improper handling of insufficient privileges in the AMD Secure Processor (ASP) could allow an attacker to provide an input value to a function without sufficient privileges and successfully write data, potentially resulting in loss of integrity of availability.	N/A	More Details
CVE-2025-48516	Insecure default configuration state of DDR5 memory module by AGESA Bootloader Firmware could allow an attacker with local user privilege to abuse the unprotected PMIC interface to create a permanent denial of service condition or affect the integrity of the memory module.	N/A	More Details
CVE-2025-48513	Use of uninitialized resource within the AMD Platform Management Framework (PMF) could allow an attacker to read a uninitialized kernel memory resulting in loss of confidentiality or availability.	N/A	More Details
CVE-2025-29944	A buffer overflow vulnerability within AMD Sensor Fusion Hub Driver can allow a local attacker to write out of bounds, potentially resulting in denial of service or crash	N/A	More Details
CVE-2025-29938	An unchecked return value within the AMD Platform Management Framework (PMF) could allow an attacker to write to an arbitrary memory address resulting in denial of service or arbitrary code execution.	N/A	More Details
CVE-2025-29937	An out of bounds read within the AMD Platform Management Framework (PMF) could allow an attacker to trigger a read of an arbitrary memory location potentially resulting in loss of availability or confidentiality.	N/A	More Details
CVE-2025-29936	Improper input validation within the AMD Platform Management Framework (PMF) could allow an attacker to unmap arbitrary memory pages potentially impacting integrity and availability, or allowing privilege escalation resulting in loss of confidentiality.	N/A	More Details
CVE-2025-29935	An out of bounds write within the AMD Platform Management Framework (PMF) could allow an attacker to execute arbitrary code at an elevated privilege level potentially leading to loss of confidentiality integrity, or availability.	N/A	More Details
CVE-2026-0481	Unrestricted IP address binding in the AMD Device Metrics Exporter (ROCm ecosystem) could allow a remote attacker to perform unauthorized changes to the GPU configuration, potentially resulting in loss of availability	N/A	More Details
CVE-2026-24662	Cross-site scripting vulnerability exists in Musetheque V4 Information Disclosure for IPKNOWLEDGE V4L1 rev2203.0 and earlier. If a file containing malicious contents is uploaded, an arbitrary script may be executed on a user's web browser when viewing the administration page showing the information of the file.	N/A	More Details
CVE-2026-28761	Cross-site request forgery vulnerability exists in Musetheque V4 Information Disclosure for IPKNOWLEDGE V4L1 rev2203.0 and earlier. If a user views a malicious page while logged-in to the affected product, unexpected operations may be done.	N/A	More Details
CVE-2026-43490	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate inherited ACE SID length smb_inherit_dacl() walks the parent directory DACL loaded from the security descriptor xattr. It verifies that each ACE contains the fixed SID header before using it, but does not verify that the variable-length SID described by sid.num_subauth is fully contained in the ACE. A malformed inheritable ACE can advertise more subauthorities than are present in the ACE. compare_sids() may then read past the ACE. smb_set_ace() also clamps the copied destination SID, but used the unchecked source SID count to compute the inherited ACE size. That could advance the temporary inherited ACE buffer pointer and nt_size accounting past the allocated buffer. Fix this by validating the parent ACE SID count and SID length before using the SID during inheritance. Compute the inherited ACE size from the copied SID so the size matches the bounded destination SID. Reject the inherited DACL if size accumulation would overflow smb_acl.size or the security descriptor allocation size.	N/A	More Details
CVE-2025-65954	SimpleSAMLphp-casserver is a CAS 1.0 and 2.0 compliant CAS server in the form of a SimpleSAMLphp module. In versions below 6.3.1 and 7.0.0, the logout endpoint accepts a url query parameter to redirect to. casserver treats that url as trusted, and either (depending on configuration) redirects the browser there, or shows a "you've been logged out" page with a link to continue to that url. Impacted configs include 'enable_logout' => true, and 'skip_logout_page' -> true. This issue has been resolved in versions 6.3.1 and 7.0.0.	N/A	More Details
CVE-2026-	A pre-authentication, code injection vulnerability in version 1.0.0 or later of the ChromaDB Python project allows an unauthenticated attacker to run arbitrary code on the server by sending a malicious model repository and trust_remote_code set to true in	N/A	More

45829	the /api/v2/tenants/{tenant}/databases/{db}/collections endpoint.		Details
CVE-2026-0983	Denial-of-service condition in M-Files Server versions before 26.5.16015.0, before 26.2 LTS, and before 25.8 LTS SR3 allows an authenticated user to cause the MFserver process to crash	N/A	More Details
CVE-2026-4320	Authorization Bypass vulnerability in Creartia's ICMS software could allow an attacker to gain unauthorized access to protected features by manipulating the HTTP redirect headers of the login process, causing the script to continue running and enabling privilege escalation without the need for credentials.	N/A	More Details
CVE-2026-6902	A vulnerability in Command-Line Client in P4 Server prior to the 2025.2 Patch 2, identified as CVE-2026-6902, has been fixed in P4 Server to address potential security risks.	N/A	More Details
CVE-2026-6050	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-45800	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.3, there is an authenticated SQL injection issue in the frontend user order history page in Vvveb CMS. A normal frontend user can log in and access /user/orders. The order_by and direction request parameters are accepted from the URL, propagated through the Orders component, and directly concatenated into the SQL ORDER BY clause in OrderSQL::getAll(). Because of this, attacker-controlled input reaches SQL structure without a whitelist or safe query construction step. This vulnerability is fixed in 1.0.8.3.	N/A	More Details
CVE-2026-45622	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.3, there is an unauthenticated reflected cross-site scripting (XSS) issue in the public product return form in Vvveb CMS. The customer_order_id POST parameter is inserted into the Order %s not found! error message when the order lookup fails, and that message is rendered in the frontend template without HTML escaping. As a result, attacker-controlled HTML/JavaScript executes in the submitting user's browser. This vulnerability is fixed in 1.0.8.3.	N/A	More Details
CVE-2026-45616	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.3, This vulnerability is fixed in 1.0.8.3.	N/A	More Details
CVE-2026-44719	Mathesar is a web application that makes working with PostgreSQL databases both simple and powerful. From 0.2.0 to before 0.10.0, collaborators.list, tables.metadata.list, explorations.list, and forms.list accept a database_id without verifying that the requesting user was a collaborator on that database. An authenticated user on the same Mathesar installation could use these methods to view Mathesar-managed metadata for databases where they were not a collaborator. Depending on the database and features in use, exposed metadata could include collaborator mappings, table metadata, saved exploration metadata, and form metadata. For forms, the exposed metadata included form tokens. For public forms, possession of the token is equivalent to possession of the public form link, which allows submission to the form under the form’s configured PostgreSQL role. This vulnerability is fixed in 0.10.0.	N/A	More Details
CVE-2026-44718	Mathesar is a web application that makes working with PostgreSQL databases both simple and powerful. From 0.2.0 to before 0.10.0, explorations.get, explorations.replace, and explorations.delete operate on an exploration_id without verifying that the requesting user was a collaborator on the exploration’s database. An authenticated user on the same Mathesar installation who knew or guessed an exploration ID could read, replace, or delete a saved exploration belonging to a database where they were not a collaborator. This affected Mathesar-managed saved exploration definitions, including names, descriptions, selected columns, display metadata, filters, sorting, and transformations. This vulnerability is fixed in 0.10.0.	N/A	More Details
CVE-2026-44699	LibJWT is a C JSON Web Token Library. From 3.0.0 to 3.3.2, libjwt accepts an RSA JWK that does not contain an alg parameter as the verification key for an HS256/HS384/HS512 token. In the OpenSSL backend, this causes HMAC verification to run with a zero-length key, so an attacker can forge a valid JWT without knowing any secret or RSA private key. This is an algorithm-confusion authentication bypass. It affects applications that load RSA keys from JWKS where alg is omitted, which is valid JWK syntax and common in real deployments, and then choose the verification algorithm from the JWT header, for example in a kid lookup callback. This vulnerability is fixed in 3.3.3.	N/A	More Details
CVE-2026-42458	Magento Long Term Support (LTS) is an unofficial, community-driven project provides an alternative to the Magento Community Edition e-commerce platform with a high level of backward compatibility. Prior to 20.18.0, there is a reflected XSS vulnerability under admin panel -> System -> Import/Export -> Dataflow - Profiles. This vulnerability is fixed in 20.18.0.	N/A	More Details
CVE-2026-42155	Magento Long Term Support (LTS) is an unofficial, community-driven project provides an alternative to the Magento Community Edition e-commerce platform with a high level of backward compatibility. Prior to 20.18.0, the XML-RPC / SOAP API session ID is generated using an outdated, time-based construction rather than a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG). All inputs to the MD5 hash are time-derived and non-secure. Because the resulting digest relies entirely on the timestamp and the PHP internal LCG state, the effective entropy is severely constrained. This violates the OWASP ASVS v4 requirement of ≥ 64 bits of entropy (V3.2.2) and NIST SP 800-63B standards. By narrowing the LCG window (via server state leaks or general predictability) and leveraging the lack of API rate-limiting, an attacker can generate a localized pool of candidate MD5 hashes and execute a high-speed online brute-force attack to hijack active API sessions. This vulnerability is fixed in 20.18.0.	N/A	More Details
CVE-2026-2031	An Improper Access Control vulnerability in several internal API endpoints for Google Cloud Application Integration prior to 2026-01-23 allows a remote, unauthenticated attacker to disclose sensitive internal information and execute arbitrary code using specially crafted HTTP requests to inadvertently exposed internal API endpoints.	N/A	More Details
CVE-2025-14972	* Countermeasures for DPA within SYMCRYPTO engine on SixG301xxx devices are not sufficiently random and will eventually repeat. * KSU keys using SYMCRYPTO will be impacted by this vulnerability.	N/A	More Details
CVE-2026-7182	Diagram's export module is vulnerable to Path Traversal in src attribute due to lack of HTML sanitization. An unauthenticated user could craft the html payload which could include local files from the server and display them in the generated pdf. This issue was fixed in version 1.1.1.	N/A	More Details
CVE-2026-44088	SzafirHost verifies the signature of the downloaded JAR file using class JarInputStream (reading from the beginning of the file), but loads classes using class JarFile/URLClassLoader (reading the Central Directory from the end). It can lead to remote code execution by allowing an attacker to combine a genuine, signed JAR file with a malicious ZIP file, causing the verification to pass but the malicious class to be loaded. This issue was fixed in version 1.2.1.	N/A	More Details

CVE-2026-8654	Improper input validation in Delphix Continuous Data connectors allows an authenticated user to execute arbitrary operating system commands on the staging or target host.	N/A	More Details
CVE-2025-0044	An out-of-bounds read in power management firmware by a malicious local attacker with low privileges could potentially lead to a partial loss of confidentiality and availability.	N/A	More Details
CVE-2025-0028	An unchecked return value within the AMD Platform Management Framework (PMF) could allow an attacker to read or modify an arbitrary address potentially resulting in loss of confidentiality, integrity, or availability.	N/A	More Details
CVE-2026-42881	STIGQter is an open-source reimplementation of DISA's STIG Viewer. From 0.1.2 to before 1.2.7, an attacker can achieve local code execution (LCE) with the privileges of the user running STIGQter. This requires user interaction: the victim must open the malicious .stigqter file and explicitly run the "Export HTML" action. This vulnerability is fixed in 1.2.7.	N/A	More Details
CVE-2026-44544	gittuf is a platform-agnostic Git security system. Prior to 0.14.0, an attacker with push access to gittuf's Reference State Log (RSL) can roll back the current policy to any previous policy trusted by the current set of root keys. gittuf determines the policy to load by inspecting the RSL. Except for the very first policy (which is automatically trusted given gittuf's TOFU model, or verified against manually specified keys), whenever an RSL entry that points to a new policy is encountered, gittuf validates that this policy is trusted. This is done by checking that the new policy's root metadata is signed by the required threshold of the current policy's root keys. Because of this, an attacker with push access to the RSL may create a new entry that references an old policy (that is trusted by the most recent policy's set of root keys), thereby rolling back gittuf's policy to the attacker's chosen state. This vulnerability is fixed in 0.14.0.	N/A	More Details
CVE-2026-42327	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.9.7 to before 0.10.79, X509Ref::ocsp_responders returns OCSP responder URLs from a certificate's AIA extension as OpensslString, whose Deref<Target = str> wraps the raw bytes with str::from_utf8_unchecked. OpenSSL does not enforce that the underlying IA5String is ASCII, so a certificate with non-UTF-8 bytes in its OCSP accessLocation causes safe Rust code to construct a &str that violates the UTF-8 invariant — resulting in undefined behavior. This vulnerability is fixed in 0.10.79.	N/A	More Details
CVE-2026-3290	Timing limitations of the HRNG in RS9116 when power save mode is enabled results in predictable values	N/A	More Details
CVE-2026-24899	Fleet is open source device management software. Prior to version 4.82.0, a vulnerability in Fleet's Windows MDM enrollment flow allows authentication tokens from any Azure AD tenant to be accepted. Because Fleet validates JWT signatures using Microsoft's multi-tenant JWKS endpoint but does not enforce the `aud` (audience) or `iss` (issuer) claims, any Microsoft-signed Azure AD access token containing the expected scopes can be used to authenticate to Fleet's MDM endpoints. If Windows MDM is enabled, an attacker with access to any Azure AD tenant can obtain a valid Microsoft-signed token and use it to enroll unauthorized devices and interact with Fleet's MDM management APIs. During device management, Fleet may expose sensitive enrollment secrets embedded in MDM command payloads, enabling further unauthorized access. Version 4.82.0 contains a patch. If an immediate upgrade is not possible, affected Fleet users should temporarily disable Windows MDM.	N/A	More Details
CVE-2026-45371	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, SiYuan publish-mode Reader can mutate Conf and SQL index via 8 ungated APIs. POST /api/graph/getGraph, POST /api/graph/getLocalGraph, POST /api/sync/setSyncInterval, POST /api/storage/updateRecentDocViewTime, POST /api/storage/updateRecentDocCloseTime, POST /api/storage/updateRecentDocOpenTime, POST /api/storage/batchUpdateRecentDocCloseTime, and POST /api/search/updateEmbedBlock are registered with model.CheckAuth only, omitting both model.CheckAdminRole and model.CheckReadonly. Each of them writes server-side state, including atomic rewrites of <workspace>/conf/conf.json via model.Conf.Save(). Any caller whose JWT passes CheckAuth, including a publish-service RoleReader (the role assigned to anonymous publish visitors) and a RoleEditor against a workspace where Editor.ReadOnly = true, can hit them This vulnerability is fixed in 3.7.0.	N/A	More Details
CVE-2026-44670	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, the kernel stores Attribute View (AV / database) names without any HTML escape, then a render template uses raw strings.ReplaceAll(tpl, "${avName}", nodeAvName) to embed the name in HTML before pushing to all clients via WebSocket. Three independent client paths (render.ts:120 → outerHTML, Title.ts:401 → innerHTML, transaction.ts:559 → innerHTML) consume the value without escaping. Because the main BrowserWindow runs nodeIntegration:true, contextIsolation:false, webSecurity:false (app/electron/main.js:407-411), HTML injection in the renderer becomes Node.js code execution. This vulnerability is fixed in 3.7.0.	N/A	More Details
CVE-2026-44588	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, he tooltip mouseover handler in app/src/block/popover.ts reads aria-label via getAttribute and passes it through decodeURIComponent before assigning to messageElement.innerHTML in app/src/dialog/tooltip.ts:41. The encoder used at the producer side, escapeAriaLabel in app/src/util/escape.ts:19-25, only handles HTML special characters (", ', <, literal <) — it leaves %XX URL-escapes untouched. So a doc title containing %3Cimg src=x onerror=...%3E round-trips through escapeAriaLabel and the HTML attribute layer unmodified. Then decodeURIComponent on the consumer side converts %3C to a literal < character (a real <, NOT a character reference). When that string is assigned to innerHTML, the HTML5 tokenizer enters TagOpenState on the literal <, parses the <img> element, and the onerror handler fires. Because the renderer runs with nodeIntegration: true, contextIsolation: false, webSecurity: false (app/electron/main.js:407-411), require('child_process') is reachable from the injected handler, escalating to arbitrary code execution.This vulnerability is fixed in 3.7.0.	N/A	More Details
CVE-2026-44522	Note Mark is an open-source note-taking application. From 0.13.0 to before 0.19.4, the Note Mark application allows authenticated users to upload assets to notes via POST /api/notes/{noteID}/assets, where the asset filename is provided through the X-Name HTTP request header. This value is stored directly in the database without any sanitization or validation - no path separator filtering, no directory traversal sequence rejection, and no use of filepath.Base() to strip directory components. The unsanitized name is persisted as-is in the note_assets table (Name column, varchar(80)). When an administrator subsequently runs the data export CLI commands (note-mark migrate export-v1 or note-mark migrate export), the stored asset name is passed directly into filepath.Join() and path.Join() calls as part of the output file path argument to os.Create(). Since Go's filepath.Join() resolves ../ sequences during path normalization, an attacker-controlled asset name containing directory traversal sequences causes the export process to write files to arbitrary locations on the filesystem, completely outside the intended export directory. This vulnerability is fixed in 0.19.4.	N/A	More Details
CVE-2026-41315	mdserver-web is a simple Linux panel. From 0.18.0 to 0.18.4, mdserver-web has a front-end unauthorized remote command execution vulnerability. Due to the lack of authentication on the /modify_crond and /start_task interfaces, it is possible to modify the default built-in scheduled tasks and start them, achieving RCE.	N/A	More Details
CVE-	CWE-312: Cleartext Storage of Sensitive Information vulnerability exists that could cause the disclosure of a sensitive information which		

2026-6332	could result in revealing protected source code and loss of confidentiality, When an authorized attacker accesses the source code for editing or compiling it.	N/A	More Details
CVE-2026-42598	Pode is a Cross-Platform PowerShell web framework for creating REST APIs, Web Sites, and TCP/SMTP servers. From 2.4.0, to before 2.13.0, when requesting content from a Static Route, it was possible to request paths such as http://localhost:8080/c:/Windows/System32/drivers/etc/hosts and have the contents returned. This vulnerability is fixed in 2.13.0.	N/A	More Details
CVE-2024-36332	Improper isolation of GPU HW register space could allow a privileged attacker in malicious Guest Virtual Machine (VM) to perform unauthorized access to specific victim range of GPU MMIO register space, potentially causing the host OS to reboot and creating a Denial of Service (DOS) condition.	N/A	More Details
CVE-2026-7805	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-3258. Reason: This candidate is a reservation duplicate of CVE-2026-3258. Notes: All CVE users should reference CVE-2026-3258instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-44515	Nextcloud News is an RSS/Atom feed reader. Prior to 28.3.0-beta.1, Nextcloud News allows authenticated users to add feeds by providing a feed URL (via the web interface or the API). In affected versions, an authenticated attacker could provide a URL pointing to internal/private IP ranges or localhost, causing the Nextcloud server to perform server-side HTTP requests to attacker-controlled destinations, but not relaying the result. This enables blind SSRF, which can be used to scan or probe internal network services that are reachable from the Nextcloud server. This vulnerability is fixed in 28.3.0-beta.1.	N/A	More Details
CVE-2026-44504	Aegra is a drop-in replacement for LangSmith Deployments. Prior to 0.9.7, with multiple authenticated users on a shared instance are vulnerable to a cross-tenant IDOR. Any authenticated attacker, given another user's thread_id, can execute graph runs against the user's thread, read the user's full checkpoint state, and inject arbitrary messages into the user's conversation history. This vulnerability is fixed in 0.9.7.	N/A	More Details
CVE-2026-44503	The RedirectHandler middleware in microsoft/kiota-java (com.microsoft.kiota:microsoft-kiota-http-okHttp v1.9.0) and other Kiota libraries fails to strip sensitive HTTP headers when following 3xx redirects to a different host or scheme. Only the Authorization header is removed; Cookie, Proxy-Authorization, and all custom headers are forwarded to the redirect target.	N/A	More Details
CVE-2026-42281	MagicMirror² is an open source modular smart mirror platform. Prior to 2.36.0, an unauthenticated Server-Side Request Forgery (SSRF) vulnerability in the /cors endpoint allows any remote attacker to force the MagicMirror² server to perform arbitrary HTTP requests to internal networks, cloud metadata services, and localhost services. The endpoint also expands environment variable placeholders (**VAR_NAME**), enabling exfiltration of server-side secrets. This vulnerability is fixed in 2.36.0.	N/A	More Details
CVE-2026-42159	Flowsint is an open-source OSINT graph exploration tool designed for cybersecurity investigation, transparency, and verification. Prior to 1.2.3, Flowsint allows a user to create investigations, which are used to manage sketches and analyses. Sketches have controllable graphs, which are comprised of nodes and relationships. The sketches contain information on an OSINT target (usernames, websites, etc) within these nodes and relationships. A remote attacker can create a node with a malicious description that contains arbitrary HTML. When the node is selected, it will render the arbitrary HTML, potentially triggering stored XSS. This vulnerability is fixed in 1.2.3.	N/A	More Details
CVE-2026-44484	PyTorch Lightning is a deep learning framework to pretrain and finetune AI models. Versions 2.6.2 and 2.6.2 have introduced functionality consistent with a credential harvesting mechanism.	N/A	More Details
CVE-2026-44371	Open OnDemand is an open-source high-performance computing portal. Prior to 4.0.11, 4.1.5, and 4.2.2, specially crafted filenames can execute javascript in the file browser This vulnerability is fixed in 4.0.11, 4.1.5, and 4.2.2.	N/A	More Details
CVE-2026-44308	Spring Cloud AWS simplifies using AWS managed services in a Spring and Spring Boot applications. From 3.0.0 to 4.0.1, pplications using Spring Cloud AWS SNS HTTP/HTTPS endpoint support (@NotificationMessageMapping, @NotificationSubscriptionMapping, @NotificationUnsubscribeConfirmationMapping) did not verify the signature of incoming SNS messages. An unauthenticated attacker who knows the endpoint URL could send crafted HTTP POST requests mimicking SNS Notification or SubscriptionConfirmation messages. This vulnerability is fixed in 4.0.2.	N/A	More Details
CVE-2026-42847	ClipBucket v5 is an open source video sharing platform. Prior to 5.5.3 - #122, there is a critical SQL Injection (SQLi) vulnerability in ClipBucket, exploitable through the type parameter on the authenticated admin endpoint admin_area/action_logs.php. The endpoint admin_area/action_logs.php reads $_GET['type'], stores it in $result_array['type'], and forwards it into fetch_action_logs(), where the value is concatenated directly into a SQL WHERE condition on action_type without parameterization. This allows UNION-based SQL injection and direct data exfiltration from the database. This vulnerability is fixed in 5.5.3 - #122.	N/A	More Details
CVE-2025-61971	Missing lock bit protection for NBIO registers could allow a local admin-privileged attacker to modify MMIO routing configurations, potentially resulting in loss of SEV-SNP guest integrity.	N/A	More Details
CVE-2026-44662	rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.10.0 to before 0.10.79, CipherCtxRef::cipher_update, CipherCtxRef::cipher_update_vec, and symm::Crypter::update incorrectly sized output buffers when used with AES key-wrap-with-padding ciphers (EVP_aes_{128,192,256}_wrap_pad). For a non-multiple-of-8 input, OpenSSL writes up to 7 bytes past the end of the caller's buffer or Vec, producing attacker-controllable heap corruption when the plaintext length is attacker-influenced. This only impacts users using AES key-wrap-with-padding ciphers. This vulnerability is fixed in 0.10.79.	N/A	More Details
CVE-2026-44666	HRConvert2 is a self-hosted, drag-and-drop & nosql file conversion server & share tool. Prior to 3.3.8, the sanitizeString() function in convertCore.php is missing backtick (`) and tab (\t) from its strip list. User input then reaches shell_exec(), where the shell interprets these characters and commands within filenames execute. This vulnerability is fixed in 3.3.8.	N/A	More Details
CVE-2024-21962	Improper Input Validation in the AMD RAID driver could allow an attacker to point to an arbitrary memory location potentially resulting in privilege escalation and arbitrary code execution.	N/A	More Details
CVE-2023-31317	Improper restriction of operations within the bounds of a memory buffer in the AMD secure processer (ASP) could allow an attacker to read or write to protected memory potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2023-31316	Improperly preserved integrity of hardware configuration state during a power save/restore operation in the AMD Secure Processor (ASP) could allow an attacker with the ability to write outside the trusted memory range (TMR) to change the execution flow of the Video Core Next (VCN) firmware potentially impacting confidentiality, integrity, or availability.	N/A	More Details

CVE-2023-31309	Improper validation in Power Management Firmware (PMFW) may allow an attacker with privileges to pass malformed workload arguments when exporting table data from SMU to DRAM potentially resulting in a loss of confidentiality and/or availability.	N/A	More Details
CVE-2022-23826	A TOCTOU (Time-Of-Check to Time-Of-Use) in the graphics interface may allow an attacker to load registers repeatedly creating a race condition potentially leading to a loss of integrity.	N/A	More Details
CVE-2021-26380	A compromised Trusted OS (TOS) driver could issue a malformed call that could potentially allow memory access outside the intended range resulting in loss of integrity.	N/A	More Details
CVE-2026-0438	A System Management Mode (SMM) handler could perform a callout to code located in non-SMM/untrusted memory. A highly privileged attacker could, with active user interaction and under high complexity and present preconditions, trigger execution of attacker-controlled code in SMM, potentially compromising the system’s confidentiality, integrity, and availability.	N/A	More Details
CVE-2026-0432	Incorrect default permissions in the installation directory for the AMD chipset driver could allow an attacker to achieve privilege escalation resulting in arbitrary code execution.	N/A	More Details
CVE-2025-52540	An improper input validation vulnerability within the AMD Platform Management Framework (PMF) Driver can allow a local attacker to write Out-of-Bounds, potentially resulting in privilege escalation.	N/A	More Details
CVE-2025-48521	Improper input validation in the AMD Secure Processor (ASP) PCI driver could allow a local attacker to trigger a Use-After-Free (UAF) condition, potentially resulting in a loss of platform integrity or crash.	N/A	More Details
CVE-2025-48520	An improper input validation vulnerability within the AMD Platform Management Framework (PMF) driver can allow a local attacker to read Out-of-Bounds potentially resulting in information disclosure or a crash	N/A	More Details
CVE-2025-48519	An improper input validation vulnerability within the AMD Platform Management Framework (PMF) driver can allow a local attacker to read or write Out-of-Bounds, potentially resulting in privilege escalation	N/A	More Details
CVE-2025-48512	Incorrect default permissions in the installation directory for the AMD general-purpose input/output controller (GPIO) could allow an attacker to achieve privilege escalation resulting in arbitrary code execution.	N/A	More Details
CVE-2025-0045	Improper Input validation in the AMD Secure Processor (ASP) PCI driver may allow a local attacker to create a buffer overflow condition, potentially resulting in a crash or denial of service	N/A	More Details
CVE-2024-36345	Improper input validation in the AMD OverDrive (AOD) System Management Mode (SMM) module could allow a privileged attacker to perform an out-of-bounds read, potentially resulting in loss of confidentiality.	N/A	More Details
CVE-2026-44427	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. From 1.1.0 to 1.7.4, the TrailingSlashMiddleware in internal/api/server.go is vulnerable to an open redirect attack. An attacker can craft a URL with a protocol-relative path (e.g., //evil.com/) that, after trailing slash removal, results in a Location header of //evil.com — which browsers interpret as an absolute URL to an external domain. This vulnerability is fixed in 1.7.5.	N/A	More Details
CVE-2026-44700	Elixir WebRTC is an Elixir implementation of the W3C WebRTC API. Prior to 0.15.1 and 0.16.1, missing DTLS peer certificate fingerprint validation in the DTLS client (active) role removes one side of WebRTC's mutual authentication. The bug is not independently exploitable for media interception in standard deployments, but enables a full man-in-the-middle attack when chained with insecure signalling or a peer with similar validation gaps. This vulnerability is fixed in 0.15.1 and 0.16.1.	N/A	More Details
CVE-2026-44679	Tuist is a virtual platform team for Swift app devs. Prior to 1.180.10, the forgot password flow allows an unauthenticated attacker to repeatedly trigger password reset emails for a known account without server-side throttling. In self-hosted deployments, this can be abused to send large volumes of unwanted email and consume downstream email delivery resources. This vulnerability is fixed in 1.180.10.	N/A	More Details
CVE-2026-44678	Tuist is a virtual platform team for Swift app devs. In 1.180.8 and earlier, the DELETE /api/projects/{account_handle}/{project_handle}/previews/{preview_id} endpoint loads the preview by its UUID without verifying that the preview belongs to the project resolved from the URL path. The route's project-level authorization plug (AuthorizationPlug, :preview) authorizes the caller against the project encoded in account_handle/project_handle — which the attacker controls — and then the action deletes whichever preview's UUID is supplied. The check therefore guards the wrong project.	N/A	More Details
CVE-2026-8495	Missing Authorization vulnerability in Drupal Date iCal allows Forceful Browsing. This issue affects Date iCal: from 0.0.0 before 4.0.15.	N/A	More Details