SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 April 2026

Generated on 22 April 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-2025-15638	Net::Dropbear versions before 0.14 for Perl contains a vulnerable version of libtomcrypt. Net::Dropbear versions before 0.14 includes versions of Dropbear 2019.78 or earlier. These include versions of libtomcrypt v1.18.1 or earlier, which is affected by CVE-2016-6129 and CVE-2018-12437.	10.0	More Details
CVE-2026-40911	WWBN AVideo is an open source video platform. In versions 29.0 and prior, the YPTSocket plugin's WebSocket server relays attacker-supplied JSON message bodies to every connected client without sanitizing the `msg` or `callback` fields. On the client side, `plugin/YPTSocket/script.js` contains two `eval()` sinks fed directly by those relayed fields (`json.msg.autoEvalCodeOnHTML` at line 568 and `json.callback` at line 95). Because tokens are minted for anonymous visitors and never revalidated beyond decryption, an unauthenticated attacker can broadcast arbitrary JavaScript that executes in the origin of every currently-connected user (including administrators), resulting in universal account takeover, session theft, and privileged action execution. Commit c08694bf6264eb4decceb78c711baee2609b4efd contains a fix.	10.0	More Details
CVE-2017-20230	Storable versions before 3.05 for Perl has a stack overflow. The retrieve_hook function stored the length of the class name into a signed integer but in read operations treated the length as unsigned. This allowed an attacker to craft data that could trigger the overflow.	10.0	More Details
CVE-2026-40933	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, due to unsafe serialization of stdio commands in the MCP adapter, an authenticated attacker can add an MCP stdio server with an arbitrary command, achieving command execution. The vulnerability lies in a bug in the input sanitization from the “Custom MCP” configuration in http://localhost:3000/canvas - where any user can add a new MCP, when doing so - adding a new MCP using stdio, the user can add any command, even though your code have input sanitization checks such as validateCommandInjection and validateArgsForLocalFileAccess, and a list of predefined specific safe commands - these commands, for example "npx" can be combined with code execution arguments ("-c touch /tmp/pwn") that enable direct code execution on the underlying OS. This vulnerability is fixed in 3.1.0.	9.9	More Details
CVE-2026-32604	Spinnaker is an open source, multi-cloud continuous delivery platform. In versions prior to 2026.1.0, 2026.0.1, 2025.4.2, and 2025.3.2, a bad actor can execute arbitrary commands very simply on the clouddriver pods. This can expose credentials, remove files, or inject resources easily. Versions 2026.1.0, 2026.0.1, 2025.4.2, and 2025.3.2 contain a patch. As a workaround, disable the gitrepo artifact types.	9.9	More Details
CVE-2026-32613	Spinnaker is an open source, multi-cloud continuous delivery platform. Echo like some other services, uses SPeL (Spring Expression Language) to process information - specifically around expected artifacts. In versions prior to 2026.1.0, 2026.0.1, 2025.4.2, and 2025.3.2, unlike orca, it was NOT restricting that context to a set of trusted classes, but allowing FULL JVM access. This enabled a user to use arbitrary java classes which allow deep access to the system. This enabled the ability to invoke commands, access files, etc. Versions 2026.1.0, 2026.0.1, 2025.4.2, and 2025.3.2 contain a patch. As a workaround, disable echo entirely.	9.9	More Details
CVE-2026-41329	OpenClaw before 2026.3.31 contains a sandbox bypass vulnerability allowing attackers to escalate privileges via heartbeat context inheritance and senderIsOwner parameter manipulation. Attackers can exploit improper context validation to bypass sandbox restrictions and achieve unauthorized privilege escalation.	9.9	More Details
	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, the external engine plugin loader concatenates a user-supplied engine name into a filesystem path without filtering path		

CVE-2026-40342	separators or .. components. An authenticated user with CREATE FUNCTION privileges can use a crafted ENGINE name to load an arbitrary shared library from anywhere on the filesystem via path traversal. The library's initialization code executes immediately during loading, before Firebird validates the module, achieving code execution as the server's OS account. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	9.9	More Details
CVE-2026-30269	Improper access control in Doorman v0.1.0 and v1.0.2 allows any authenticated user to update their own account role to a non-admin privileged role via /platform/user/{username}. The `role` field is accepted by the update model without a manage_users permission check for self-updates, enabling privilege escalation to high-privileged roles.	9.9	More Details
CVE-2026-20186	A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	9.9	More Details
CVE-2026-39842	OpenRemote is an open-source IoT platform. Versions 1.21.0 and below contain two interrelated expression injection vulnerabilities in the rules engine that allow arbitrary code execution on the server. The JavaScript rules engine executes user-supplied scripts via Nashorn's ScriptEngine.eval() without sandboxing, class filtering, or access restrictions, and the authorization check in RulesResourceImpl only restricts Groovy rules to superusers while leaving JavaScript rules unrestricted for any user with the write:rules role. Additionally, the Groovy rules engine has a GroovyDenyAllFilter security filter that is defined but never registered, as the registration code is commented out, rendering the SandboxTransformer ineffective for superuser-created Groovy rules. A non-superuser attacker with the write:rules role can create JavaScript rulesets that execute with full JVM access, enabling remote code execution as root, arbitrary file read, environment variable theft including database credentials, and complete multi-tenant isolation bypass to access data across all realms. This issue has been fixed in version 1.22.0.	9.9	More Details
CVE-2026-20180	A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	9.9	More Details
CVE-2026-20147	A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	9.9	More Details
CVE-2026-40906	Electric is a Postgres sync engine. From 1.1.12 to before 1.5.0, the order_by parameter in the ElectricSQL /v1/shape API is vulnerable to error-based SQL injection, allowing any authenticated user to read, write, and destroy the full contents of the underlying PostgreSQL database through crafted ORDER BY expressions. This vulnerability is fixed in 1.5.0.	9.9	More Details
CVE-2026-40494	SAIL is a cross-platform library for loading and saving images with support for animation, metadata, and ICC profiles. Prior to commit 45d48d1f2e8e0d73e80bc1fd5310cb57f4547302, the TGA codec's RLE decoder in `tga.c` has an asymmetric bounds check vulnerability. The run-packet path (line 297) correctly clamps the repeat count to the remaining buffer space, but the raw-packet path (line 305-311) has no equivalent bounds check. This allows writing up to 496 bytes of attacker-controlled data past the end of a heap buffer. Commit 45d48d1f2e8e0d73e80bc1fd5310cb57f4547302 patches the issue.	9.8	More Details
CVE-2026-25917	Dag Authors, who normally should not be able to execute code in the webserver context could craft XCom payload causing the webserver to execute arbitrary code. Since Dag Authors are already highly trusted, severity of this issue is Low. Users are recommended to upgrade to Apache Airflow 3.2.0, which fixes the issue.	9.8	More Details
CVE-2026-29649	NEMU contains an implementation flaw in its RISC-V Hypervisor CSR handling where henvcfg[7:4] (CBIE/CBCFE/CBZE-related fields) is incorrectly masked/updated based on menvcfg[7:4], so a machine-mode write to menvcfg can implicitly modify the hypervisor's environment configuration. This can lead to incorrect enforcement of virtualization configuration and may cause unexpected traps or denial of service when executing cache-block management instructions in virtualized contexts (V=1).	9.8	More Details
CVE-2026-5963	EasyFlow .NET developed by Digiwin has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2026-5964	EasyFlow .NET developed by Digiwin has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2026-5760	SGLang's reranking endpoint (/v1/rerank) achieves Remote Code Execution (RCE) when a model file containing a malicious tokenizer.chat_template is loaded, as the Jinja2 chat templates are rendered using an unsandboxed jinja2.Environment().	9.8	More Details
CVE-2026-	Vvveb prior to 1.0.8.1 contains a code injection vulnerability in the installation endpoint where the subdir POST parameter is written unsanitized into the env.php configuration file without escaping or validation. Attackers can		

39918	inject arbitrary PHP code by breaking out of the string context in the define statement to achieve unauthenticated remote code execution as the web server user.	9.8	More Details
CVE-2026-40492	SAIL is a cross-platform library for loading and saving images with support for animation, metadata, and ICC profiles. Prior to commit 36aa5c7ec8a2bb35f6fb867a1177a6f141156b02, the XWD codec resolves pixel format based on `pixmap_depth` but the byte-swap code uses `bits_per_pixel` independently. When `pixmap_depth=8` (BPP8_INDEXED, 1 byte/pixel buffer) but `bits_per_pixel=32`, the byte-swap loop accesses memory as `uint32_t*`, reading/writing 4x the allocated buffer size. This is a different vulnerability from the previously reported GHSA-3g38-x2pj-mv55 (CVE-2026-27168), which addressed `bytes_per_line` validation. Commit 36aa5c7ec8a2bb35f6fb867a1177a6f141156b02 contains a patch.	9.8	More Details
CVE-2026-32956	SD-330AC and AMC Manager provided by silex technology, Inc. contain a heap-based buffer overflow vulnerability in processing the redirect URLs. Arbitrary code may be executed on the device.	9.8	More Details
CVE-2026-5965	NewSoftOA developed by NewSoft has an OS Command Injection vulnerability, allowing unauthenticated local attackers to inject arbitrary OS commands and execute them on the server.	9.8	More Details
CVE-2026-29646	In OpenXiangShan NEMU prior to 55295c4, when running with RVH (Hypervisor extension) enabled, a VS-mode guest write to the supervisor interrupt-enable CSR (sie) may be handled incorrectly and can influence machine-level interrupt enable state (mie). This breaks privilege/virtualization isolation and can lead to denial of service or privilege-boundary violation in environments relying on NEMU for correct interrupt virtualization.	9.8	More Details
CVE-2026-5450	Calling the scanf family of functions with a %mc (malloc'd character match) in the GNU C Library version 2.7 to version 2.43 with a format width specifier with an explicit width greater than 1024 could result in a one byte heap buffer overflow.	9.8	More Details
CVE-2026-6748	Uninitialized memory in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	9.8	More Details
CVE-2026-6768	Mitigation bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	9.8	More Details
CVE-2026-6771	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	9.8	More Details
CVE-2026-40050	CrowdStrike has released security updates to address a critical unauthenticated path traversal vulnerability (CVE-2026-40050) in LogScale. This vulnerability only requires mitigation by customers that host specific versions of LogScale and does not affect Next-Gen SIEM customers. The vulnerability exists in a specific cluster API endpoint that, if exposed, allows a remote attacker to read arbitrary files from the server filesystem without authentication. Next-Gen SIEM customers are not affected and do not need to take any action. CrowdStrike mitigated the vulnerability for LogScale SaaS customers by deploying network-layer blocks to all clusters on April 7, 2026. We have proactively reviewed all log data and there is no evidence of exploitation. LogScale Self-hosted customers should upgrade to a patched version immediately to remediate the vulnerability. CrowdStrike identified this vulnerability during continuous and ongoing product testing.	9.8	More Details
CVE-2026-40884	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.6, goshs contains an SFTP authentication bypass when the documented empty-username basic-auth syntax is used. If the server is started with -b ':pass' together with -sftp, goshs accepts that configuration but does not install any SFTP password handler. As a result, an unauthenticated network attacker can connect to the SFTP service and access files without a password. This vulnerability is fixed in 2.0.0-beta.6.	9.8	More Details
CVE-2026-33518	An incorrect privilege assignment vulnerability exists in Esri Portal for ArcGIS 11.5 in Windows and Linux that allows highly privileged users to create developer credentials that may grant more privileges than expected.	9.8	More Details
CVE-2026-33519	An incorrect authorization vulnerability exists in Esri Portal for ArcGIS 11.4, 11.5 and 12.0 on Windows, Linux and Kubernetes that did not correctly check permissions assigned to developer credentials.	9.8	More Details
CVE-2026-34275	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: Setup and Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in takeover of Oracle Advanced Inbound Telephony. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-40351	FastGPT is an AI Agent building platform. In versions prior to 4.14.9.5, the password-based login endpoint uses TypeScript type assertion without runtime validation, allowing an unauthenticated attacker to pass a MongoDB query operator object (e.g., {"$ne": ""}) as the password field. This NoSQL injection bypasses the password check, enabling login as any user including the root administrator. This issue has been fixed in version 4.14.9.5.	9.8	More Details
CVE-2026-1555	The WebStack theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the io_img_upload() function in all versions up to, and including, 1.2024. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2026-31843	The goodoneuz/pay-uz Laravel package (<= 2.2.24) contains a critical vulnerability in the /payment/api/editable/update endpoint that allows unauthenticated attackers to overwrite existing PHP payment hook files. The endpoint is exposed via Route::any() without authentication middleware, enabling remote access without credentials. User-controlled input is directly written into executable PHP files using file_put_contents(). These files are later executed via require() during normal payment processing workflows, resulting in remote code execution under default application behavior. The payment secret token mentioned by the vendor is unrelated to this endpoint and does not mitigate the vulnerability.	9.8	More Details

CVE-2026-33082	DataEase is an open source data visualization analysis tool. Versions 2.10.20 and below contain a SQL injection vulnerability in the dataset export functionality. The expressionTree parameter in POST /de2api/datasetTree/exportDataset is deserialized into a filtering object and passed to WhereTree2Str.transFilterTrees for SQL translation, where user-controlled values in "like" filter terms are directly concatenated into SQL fragments without sanitization. An attacker can inject arbitrary SQL commands by escaping the string literal in the filter value, enabling blind SQL injection through techniques such as time-based extraction of database information. This issue has been fixed in version 2.10.21.	9.8	More Details
CVE-2026-3461	The Visa Acceptance Solutions plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.1.0. This is due to the `express_pay_product_page_pay_for_order()` function logging users in based solely on a user-supplied billing email address during guest checkout for subscription products, without verifying email ownership, requiring a password, or validating a one-time token. This makes it possible for unauthenticated attackers to log in as any existing user, including administrators, by providing the target user's email address in the billing_details parameter, resulting in complete account takeover and site compromise.	9.8	More Details
CVE-2026-30625	Upsonic 0.71.6 contains a remote code execution vulnerability in its MCP server/task creation functionality. The application allows users to define MCP tasks with arbitrary command and args values. Although an allowlist exists, certain allowed commands (npm, npx) accept argument flags that enable execution of arbitrary OS commands. Maliciously crafted MCP tasks may lead to remote code execution with the privileges of the Upsonic process. In version 0.72.0 Upsonic added a warning about using Stdio servers being able to execute commands directly on the machine.	9.8	More Details
CVE-2026-20184	A vulnerability in the integration of single sign-on (SSO) with Control Hub in Cisco Webex Services could have allowed an unauthenticated, remote attacker to impersonate any user within the service. This vulnerability existed because of improper certificate validation. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by connecting to a service endpoint and supplying a crafted token. A successful exploit could have allowed the attacker to gain unauthorized access to legitimate Cisco Webex services.	9.8	More Details
CVE-2026-30993	Slah CMS v1.5.0 and below was discovered to contain a remote code execution (RCE) vulnerability in the session() function at config.php. This vulnerability is exploitable via a crafted input.	9.8	More Details
CVE-2026-4880	The Barcode Scanner (+Mobile App) – Inventory manager, Order fulfillment system, POS (Point of Sale) plugin for WordPress is vulnerable to privilege escalation via insecure token-based authentication in all versions up to, and including, 1.11.0. This is due to the plugin trusting a user-supplied Base64-encoded user ID in the token parameter to identify users, leaking valid authentication tokens through the 'barcodeScannerConfigs' action, and lacking meta-key restrictions on the 'setUserMeta' action. This makes it possible for unauthenticated attackers to escalate their privileges to that of an administrator by first spoofing the admin user ID to leak their authentication token, then using that token to update any user's 'wp_capabilities' meta to gain full administrative access.	9.8	More Details
CVE-2026-40504	Creolabs Gravity before 0.9.6 contains a heap buffer overflow vulnerability in the gravity_vm_exec function that allows attackers to write out-of-bounds memory by crafting scripts with many string literals at global scope. Attackers can exploit insufficient bounds checking in gravity_fiber_reassign() to corrupt heap metadata and achieve arbitrary code execution in applications that evaluate untrusted scripts.	9.8	More Details
CVE-2026-6350	MailGates/MailAudit developed by Openfind has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and execute arbitrary code.	9.8	More Details
CVE-2026-3596	The Riaxe Product Customizer plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.1.2. The plugin registers an unauthenticated AJAX action ('wp_ajax_nopriv_install-imprint') that maps to the ink_pd_add_option() function. This function reads 'option' and 'opt_value' from $_POST, then calls delete_option() followed by add_option() using these attacker-controlled values without any nonce verification, capability checks, or option name allowlist. This makes it possible for unauthenticated attackers to update arbitrary WordPress options, which can be leveraged for privilege escalation by enabling user registration and setting the default user role to administrator.	9.8	More Details
CVE-2026-35546	Anviz CX2 Lite and CX7 are vulnerable to unauthenticated firmware uploads. This causes crafted archives to be accepted, enabling attackers to plant and execute code and obtain a reverse shell.	9.8	More Details
CVE-2026-37339	SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_genre.php.	9.8	More Details
CVE-2026-37340	SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/edit_music.php.	9.8	More Details
CVE-2026-37345	SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/manage_park.php.	9.8	More Details
CVE-2026-40493	SAIL is a cross-platform library for loading and saving images with support for animation, metadata, and ICC profiles. Prior to commit c930284445ea3ff94451ccd7a57c999eca3bc979, the PSD codec computes bytes-per-pixel (`bpp`) from raw header fields `channels * depth`, but the pixel buffer is allocated based on the resolved pixel format. For LAB mode with `channels=3, depth=16`, `bpp = (3*16+7)/8 = 6`, but the format `BPP40_CIE_LAB` allocates only 5 bytes per pixel. Every pixel write overshoots, causing a deterministic heap buffer overflow on every row. Commit c930284445ea3ff94451ccd7a57c999eca3bc979 contains a patch.	9.8	More Details
CVE-2026-6443	All plugins by Essentialplugin for WordPress are vulnerable to an injected backdoor in various versions. This is due to the plugin being sold to a malicious threat actor that embedded a backdoor in all of the plugin's they acquired. This makes it possible for the threat actor to maintain a persistent backdoor and inject spam into the affected sites.	9.8	More Details
	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the API datasource update process. When a new table definition is added during a datasource update via /de2api/datasource/update, the deTableName field from the user-submitted configuration is		

CVE-2026-33122	passed to DatasourceSyncManage.createEngineTable, where it is substituted into a CREATE TABLE statement template without any sanitization or identifier escaping. An authenticated attacker can inject arbitrary SQL commands by crafting a deTableName that breaks out of identifier quoting, enabling error-based SQL injection that can extract database information. This issue has been fixed in version 2.10.21.	9.8	More Details
CVE-2026-37749	A SQL injection vulnerability in CodeAstro Simple Attendance Management System v1.0 allows remote unauthenticated attackers to bypass authentication via the username parameter in index.php.	9.8	More Details
CVE-2026-34018	An SQL injection vulnerability exists in CubeCart prior to 6.6.0, which may allow an attacker to execute an arbitrary SQL statement on the product.	9.8	More Details
CVE-2026-6296	Heap buffer overflow in ANGLE in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-40173	Dgraph is an open source distributed GraphQL database. Versions 25.3.1 and prior contain an unauthenticated credential disclosure vulnerability where the /debug/pprof/cmdline endpoint is registered on the default mux and reachable without authentication, exposing the full process command line including the admin token configured via the --security "token=..." startup flag. An attacker can retrieve the leaked token and reuse it in the X-Dgraph-AuthToken header to gain unauthorized access to admin-only endpoints such as /admin/config/cache_mb, bypassing the adminAuthHandler token validation. This enables unauthorized privileged administrative access including configuration changes and operational control actions in any deployment where the Alpha HTTP port is reachable by untrusted parties. This issue has been fixed in version 25.3.2.	9.4	More Details
CVE-2026-37338	SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_user.php.	9.4	More Details
CVE-2026-40576	excel-mcp-server is a Model Context Protocol server for Excel file manipulation. A path traversal vulnerability exists in excel-mcp-server versions up to and including 0.1.7. When running in SSE or Streamable-HTTP transport mode (the documented way to use this server remotely), an unauthenticated attacker on the network can read, write, and overwrite arbitrary files on the host filesystem by supplying crafted filepath arguments to any of the 25 exposed MCP tool handlers. The server is intended to confine file operations to a directory set by the EXCEL_FILES_PATH environment variable. The function responsible for enforcing this boundary — get_excel_path() — fails to do so due to two independent flaws: it passes absolute paths through without any check, and it joins relative paths without resolving or validating the result. Combined with zero authentication on the default network-facing transport and a default bind address of 0.0.0.0 (all interfaces), this allows trivial remote exploitation. This vulnerability is fixed in 0.1.8.	9.4	More Details
CVE-2026-39109	SQL Injection vulnerability in Apartment Visitors Management System Apartment Visitors Management System V1.1 within the username parameter of the login page (index.php). This allows an unauthenticated attacker to manipulate backend SQL queries during authentication and retrieve sensitive database contents.	9.4	More Details
CVE-2026-40959	Luanti 5 before 5.15.2, when LuaJIT is used, allows a Lua sandbox escape via a crafted mod.	9.3	More Details
CVE-2026-40317	NovumOS is a custom 32-bit operating system written in Zig and x86 Assembly. In versions prior to 0.24, Syscall 12 (JumpToUser) accepts an arbitrary entry point address from user-space registers without validation, allowing any Ring 3 user-mode process to jump to kernel addresses and execute arbitrary code in Ring 0 context, resulting in local privilege escalation. This issue has been fixed in version 0.24. If developers are unable to immediately update, they should restrict syscall access by running the system in single-user mode without Ring 3, and disable user-mode processes by only running kernel shell with no user processes. This issue has been fixed in version 0.24.	9.3	More Details
CVE-2026-34285	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-34279	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-41193	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, FreeScout's module installation feature extracts ZIP archives without validating file paths, allowing an authenticated admin to write files arbitrarily on the server filesystem via a specially crafted ZIP. Version 1.8.215 fixes the vulnerability.	9.1	More Details
CVE-2026-34286	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the database backup restore		

CVE-2026-40484	functionality extracts uploaded archive contents and copies files from the Images/ directory into the web-accessible document root using recursiveCopyDirectory(), which performs no file extension filtering. An authenticated administrator can upload a crafted backup archive containing a PHP webshell inside the Images/ directory, which is then written to a publicly accessible path and executable via HTTP requests, resulting in remote code execution as the web server user. The restore endpoint also lacks CSRF token validation, enabling exploitation through cross-site request forgery targeting an authenticated administrator. This issue has been fixed in version 7.2.0.	9.1	More Details
CVE-2026-40903	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.6, goshs has an ArtiPACKED vulnerability. ArtiPACKED can lead to leakage of the GITHUB_TOKEN through workflow artifacts, even though the token is not present in the repository source code. This vulnerability is fixed in 2.0.0-beta.6.	9.1	More Details
CVE-2026-40887	Vendure is an open-source headless commerce platform. Starting in version 1.7.4 and prior to versions 2.3.4, 3.5.7, and 3.6.2, an unauthenticated SQL injection vulnerability exists in the Vendure Shop API. A user-controlled query string parameter is interpolated directly into a raw SQL expression without parameterization or validation, allowing an attacker to execute arbitrary SQL against the database. This affects all supported database backends (PostgreSQL, MySQL/MariaDB, SQLite). The Admin API is also affected, though exploitation there requires authentication. Versions 2.3.4, 3.5.7, and 3.6.2 contain a patch. For those who are unable to upgrade immediately, Vendure has made a hotfix available that uses `RequestContextService.getLanguageCode` to validate the `languageCode` input at the boundary. This blocks injection payloads before they can reach any query. The hotfix replaces the existing `getLanguageCode` method in `packages/core/src/service/helpers/request-context/request-context.service.ts`. Invalid values are silently dropped and the channel's default language is used instead. The patched versions additionally convert the vulnerable SQL interpolation to a parameterized query as defense in depth.	9.1	More Details
CVE-2025-41118	Pyroscope is an open-source continuous profiling database. The database supports various storage backends, including Tencent Cloud Object Storage (COS). If the database is configured to use Tencent COS as the storage backend, an attacker could extract the secret_key configuration value from the Pyroscope API. To exploit this vulnerability, an attacker needs direct access to the Pyroscope API. We highly recommend limiting the public internet exposure of all our databases, such that they are only accessible by trusted users or internal systems. This vulnerability is fixed in versions: 1.15.x: 1.15.2 and above. 1.16.x: 1.16.1 and above. 1.17.x: 1.17.0 and above (i.e. all versions). Thanks to Théo Cusnir for reporting this vulnerability to us via our bug bounty program.	9.1	More Details
CVE-2026-34287	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-33807	@fastify/express v4.0.4 and earlier contains a path handling bug in the onRegister function that causes middleware paths to be doubled when inherited by child plugins. When a child plugin is registered with a prefix that matches a middleware path, the middleware path is prefixed a second time, causing it to never match incoming requests. This results in complete bypass of Express middleware security controls, including authentication, authorization, and rate limiting, for all routes defined within affected child plugin scopes. No special configuration or request crafting is required. Upgrade to @fastify/express v4.0.5 or later.	9.1	More Details
CVE-2026-40372	Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network.	9.1	More Details
CVE-2026-40324	Hot Chocolate is an open-source GraphQL server. Prior to versions 12.22.7, 13.9.16, 14.3.1, and 15.1.14, Hot Chocolate's recursive descent parser `Utf8GraphQLParser` has no recursion depth limit. A crafted GraphQL document with deeply nested selection sets, object values, list values, or list types can trigger a `StackOverflowException` on payloads as small as 40 KB. Because `StackOverflowException` is uncatchable in .NET (since .NET 2.0), the entire worker process is terminated immediately. All in-flight HTTP requests, background `IHostedService` tasks, and open WebSocket subscriptions on that worker are dropped. The orchestrator (Kubernetes, IIS, etc.) must restart the process. This occurs before any validation rules run — `MaxExecutionDepth`, complexity analyzers, persisted query allow-lists, and custom `IDocumentValidatorRule` implementations cannot intercept the crash because `Utf8GraphQLParser.Parse` is invoked before validation. The `MaxAllowedFields=2048` limit does not help because the crashing payloads contain very few fields. The fix in versions 12.22.7, 13.9.16, 14.3.1, and 15.1.14 adds a `MaxAllowedRecursionDepth` option to `ParserOptions` with a safe default, and enforces it across all recursive parser methods (`ParseSelectionSet`, `ParseValueLiteral`, `ParseObject`, `ParseList`, `ParseTypeReference`, etc.). When the limit is exceeded, a catchable `SyntaxException` is thrown instead of overflowing the stack. There is no application-level workaround. `StackOverflowException` cannot be caught in .NET. The only mitigation is to upgrade to a patched version. Operators can reduce (but not eliminate) risk by limiting HTTP request body size at the reverse proxy or load balancer layer, though the smallest crashing payload (40 KB) is well below most default body size limits and is highly compressible (~few hundred bytes via gzip).	9.1	More Details
CVE-2026-33557	A possible security vulnerability has been identified in Apache Kafka. By default, the broker property `sasl.oauthbearer.jwt.validator.class` is set to `org.apache.kafka.common.security.oauthbearer.DefaultJwtValidator`. It accepts any JWT token without validating its signature, issuer, or audience. An attacker can generate a JWT token from any issuer with the `preferred_username` set to any user, and the broker will accept it. We advise the Kafka users using kafka v4.1.0 or v4.1.1 to set the config `sasl.oauthbearer.jwt.validator.class` to `org.apache.kafka.common.security.oauthbearer.BrokerJwtValidator` explicitly to avoid this vulnerability. Since Kafka v4.1.2 and v4.2.0 and later, the issue is fixed and will correctly validate the JWT token.	9.1	More Details
CVE-2026-6388	A flaw was found in ArgoCD Image Updater. This vulnerability allows an attacker, with permissions to create or modify an ImageUpdater resource in a multi-tenant environment, to bypass namespace boundaries. By exploiting insufficient validation, the attacker can trigger unauthorized image updates on applications managed by other tenants. This leads to cross-namespace privilege escalation, impacting application integrity through unauthorized application updates.	9.1	More Details

CVE-2026-40525	OpenViking prior to version 0.3.9 contains an authentication bypass vulnerability in the VikingBot OpenAPI HTTP route surface where the authentication check fails open when the api_key configuration value is unset or empty. Remote attackers with network access to the exposed service can invoke privileged bot-control functionality without providing a valid X-API-Key header, including submitting attacker-controlled prompts, creating or using bot sessions, and accessing downstream tools, integrations, secrets, or data accessible to the bot.	9.1	More Details
CVE-2026-6284	An attacker with network access to the PLC is able to brute force discover passwords to gain unauthorized access to systems and services. The limited password complexity and no password input limiters makes brute force password enumeration possible.	9.1	More Details
CVE-2026-5358	The obsolete nis_local_principal function in the GNU C Library version 2.43 and older may overflow a buffer in the data section, which could allow an attacker to spoof a crafted response to a UDP request generated by this function and overwrite neighboring static data in the requesting application. NIS support is obsolete and has been deprecated in the GNU C Library since version 2.26 and is only maintained for legacy usage. Applications should port away from NIS to more modern identity and access management services.	9.1	More Details
CVE-2026-6270	@fastify/middie versions 9.3.1 and earlier do not register inherited middleware directly on child plugin engine instances. When a Fastify application registers authentication middleware in a parent scope and then registers child plugins with @fastify/middie, the child scope does not inherit the parent middleware. This allows unauthenticated requests to reach routes defined in child plugin scopes, bypassing authentication and authorization checks. Upgrade to @fastify/middie 9.3.2 to fix this issue. There are no workarounds.	9.1	More Details
CVE-2026-6257	Vvveb CMS v1.0.8 contains a remote code execution vulnerability in its media management functionality where a missing return statement in the file rename handler allows authenticated attackers to rename files to blocked extensions .php or .htaccess. Attackers can exploit this logic flaw by first uploading a text file and renaming it to .htaccess to inject Apache directives that register PHP-executable MIME types, then uploading another file and renaming it to .php to execute arbitrary operating system commands as the www-data user.	9.1	More Details
CVE-2026-37347	SourceCodester Payroll Management and Information System v1.0 is vulnerable to SQL Injection in the file /payroll/view_employee.php.	9.1	More Details
CVE-2026-40258	The Gramps Web API is a Python REST API for the genealogical research software Gramps. Versions 1.6.0 through 3.11.0 have a path traversal vulnerability (Zip Slip) in the media archive import feature. An authenticated user with owner-level privileges can craft a malicious ZIP file with directory-traversal filenames to write arbitrary files outside the intended temporary extraction directory on the server's local filesystem. Startig in version 3.11.1, ZIP entry names are now validated against the resolved real path of the temporary directory before extraction. Any entry whose resolved path falls outside the temporary directory raises an error and aborts the import.	9.1	More Details
CVE-2026-5652	An insecure direct object reference vulnerability in the Users API component of Crafty Controller allows a remote, authenticated attacker to perform user modification actions via improper API permissions validation.	9.0	More Details
CVE-2026-40569	FreeScout is a free self-hosted help desk and shared mailbox. Versions prior to 1.8.213 have a mass assignment vulnerability in the mailbox connection settings endpoints of FreeScout (`connectionIncomingSave()` at `app/Http/Controllers/MailboxesController.php:468` and `connectionOutgoingSave()` at line 398). Both methods pass `$request->all()` directly to `$mailbox->fill()` without any field allowlisting, allowing an authenticated admin to overwrite any of the 32 fields in the Mailbox model's `$fillable` array -- including security-critical fields that do not belong to the connection settings form, such as `auto_bcc`, `out_server`, `out_password`, `signature`, `auto_reply_enabled`, and `auto_reply_message`. Validation in `connectionIncomingSave()` is entirely commented out, and the validator in `connectionOutgoingSave()` only checks value formats for SMTP fields without stripping extra parameters. An authenticated admin user can exploit this by appending hidden parameters (e.g., `auto_bcc=attacker@evil.com`) to a legitimate connection settings save request. Because the `auto_bcc` field is not displayed on the connection settings form (it only appears on the general mailbox settings page), the injection is invisible to other administrators reviewing connection settings. Once set, every outgoing email from the affected mailbox is silently BCC'd to the attacker via the `SendReplyToCustomer` job. The same mechanism allows redirecting outgoing SMTP through an attacker-controlled server, injecting tracking pixels or phishing links into email signatures, and enabling attacker-crafted auto-replies -- all from a single HTTP request. This is particularly dangerous in multi-admin environments where one admin can silently surveil mailboxes managed by others, and when an admin session is compromised via a separate vulnerability (e.g., XSS), the attacker gains persistent email exfiltration that survives session expiry. Version 1.8.213 fixes the issue.	9.0	More Details
CVE-2026-40572	NovumOS is a custom 32-bit operating system written in Zig and x86 Assembly. In versions prior to 0.24, Syscall 15 (MemoryMapRange) allows Ring 3 user-mode processes to map arbitrary virtual address ranges into their address space without validating against forbidden regions, including critical kernel structures such as the IDT, GDT, TSS, and page tables. A local attacker can exploit this to modify kernel interrupt handlers, resulting in privilege escalation from user mode to kernel context. This issue has been fixed in version 0.24.	9.0	More Details
CVE-2026-40478	Thymeleaf is a server-side Java template engine for web and standalone environments. Versions 3.1.3.RELEASE and prior contain a security bypass vulnerability in the the expression execution mechanisms. Although the library provides mechanisms to prevent expression injection, it fails to properly neutralize specific syntax patterns that allow for the execution of unauthorized expressions. If an application developer passes unvalidated user input directly to the template engine, an unauthenticated remote attacker can bypass the library's protections to achieve Server-Side Template Injection (SSTI). This issue has ben fixed in version 3.1.4.RELEASE.	9.0	More Details
CVE-2026-40322	SiYuan is an open-source personal knowledge management system. In versions 3.6.3 and below, Mermaid diagrams are rendered with securityLevel set to "loose", and the resulting SVG is injected into the DOM via innerHTML. This allows attacker-controlled javascript: URLs in Mermaid code blocks to survive into the rendered output. On desktop builds using Electron, windows are created with nodeIntegration enabled and contextIsolation disabled, escalating the stored XSS to arbitrary code execution when a victim opens a note containing a malicious Mermaid block and clicks the rendered diagram node. This issue has been fixed in version 3.6.4.	9.0	More Details

CVE-2026-24467	OpenAEV is an open source platform allowing organizations to plan, schedule and conduct cyber adversary simulation campaign and tests. Starting in version 1.0.0 and prior to version 2.0.13, OpenAEV's password reset implementation contains multiple security weaknesses that together allow reliable account takeover. The primary issue is that password reset tokens do not expire. Once a token is generated, it remains valid indefinitely, even if significant time has passed or if newer tokens are issued for the same account. This allows an attacker to accumulate valid password reset tokens over time and reuse them at any point in the future to reset a victim's password. A secondary weakness is that password reset tokens are only 8 digits long. While an 8-digit numeric token provides 100,000,000 possible combinations (which is secure enough), the ability to generate large numbers of valid tokens drastically reduces the required number of attempts to guess a valid password reset token. For example, if an attacker generates 2,000 valid tokens, the brute-force effort is reduced to approximately 50,000 attempts, which is a trivially achievable number of requests for an automated attack. (100 requests per second can mathematically find a valid password reset token in 500 seconds.) By combining these flaws, an attacker can mass-generate valid password reset tokens and then brute-force them efficiently until a match is found, allowing the attacker to reset the victim's password to a value of their choosing. The original password is not required, and the attack can be performed entirely without authentication. This vulnerability enables full account takeover that leads to platform compromise. An unauthenticated remote attacker can reset the password of any registered user account and gain complete access without authentication. Because user email addresses are exposed to other users by design, a single guessed or observed email address is sufficient to compromise even administrator accounts with non-guessable email addresses. This design flaw results in a reliable and scalable account takeover vulnerability that affects any registered user account in the system. Note: The vulnerability does not require OpenAEV to have the email service configured. The exploit does not depend on the target email address to be a real email address. It just needs to be registered to OpenAEV. Successful exploitation allows an unauthenticated remote attacker to access sensitive data (such as the Findings section of a simulation), modify payloads executed by deployed agents to compromise all hosts where agents are installed (therefore the Scope is changed). Users should upgrade to version 2.0.13 to receive a fix.	9.0	More Details
CVE-2026-40477	Thymeleaf is a server-side Java template engine for web and standalone environments. Versions 3.1.3.RELEASE and prior contain a security bypass vulnerability in the expression execution mechanisms. Although the library provides mechanisms to prevent expression injection, it fails to properly restrict the scope of accessible objects, allowing specific potentially sensitive objects to be reached from within a template. If an application developer passes unvalidated user input directly to the template engine, an unauthenticated remote attacker can bypass the library's protections to achieve Server-Side Template Injection (SSTI). This issue has ben fixed in version 3.1.4.RELEASE.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-40899	A Stored Cross-Site Scripting vulnerability was discovered in the Assets and Nodes functionality due to improper validation of an input parameter. An authenticated user with custom fields privileges can define a malicious custom field containing a JavaScript payload. When the victim views the Assets or Nodes pages, the XSS executes in their browser context, allowing the attacker to perform unauthorized actions as the victim, such as modify application data, disrupt application availability, and access limited sensitive information.	8.9	More Details
CVE-2026-40487	Postiz is an AI social media scheduling tool. Prior to version 2.21.6, a file upload validation bypass allows any authenticated user to upload arbitrary HTML, SVG, or other executable file types to the server by spoofing the `Content-Type` header. The uploaded files are then served by nginx with a Content-Type derived from their original extension (`text/html`, `image/svg+xml`), enabling Stored Cross-Site Scripting (XSS) in the context of the application's origin. This can lead to session riding, account takeover, and full compromise of other users' accounts. Version 2.21.6 contains a fix.	8.9	More Details
CVE-2026-40901	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below ship the legacy velocity-1.7.jar, which pulls in commons-collections-3.2.1.jar containing the InvokerTransformer deserialization gadget chain. Quartz 2.3.2, also bundled in the application, deserializes job data BLOBs from the qrtz_job_details table using ObjectInputStream with no deserialization filter or class allowlist. An authenticated attacker who can write to the Quartz job table, such as through the previously described SQL injection in previewSql, can replace a scheduled job's JOB_DATA with a malicious CommonsCollections6 gadget chain payload. When the Quartz cron trigger fires, the payload is deserialized and executes arbitrary commands as root inside the container, achieving full remote code execution. This issue has been fixed in version 2.10.21.	8.8	More Details
CVE-2026-6299	Use after free in Prerender in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-35582	Emissary is a P2P based data-driven workflow engine. In versions 8.42.0 and below, Executrix.getCommand() is vulnerable to OS command injection because it interpolates temporary file paths into a /bin/sh -c shell command string without any escaping or input validation. The IN_FILE_ENDING and OUT_FILE_ENDING configuration keys flow directly into these paths, allowing a place author who can write or modify a .cfg file to inject arbitrary shell metacharacters that execute OS commands in the JVM process's security context. The framework already sanitizes placeName via an allowlist before embedding it in the same shell string, but applies no equivalent sanitization to file ending values. No runtime privileges beyond place configuration authorship, and no API or network access, are required to exploit this vulnerability. This is a framework-level defect with no safe mitigation available to downstream implementors, as Executrix provides neither escaping nor documented preconditions against metacharacters in file ending inputs. This issue has been fixed in version 8.43.0.	8.8	More Details
CVE-2026-40350	Movary is a self hosted web app to track and rate a user's watched movies. Prior to version 0.71.1, an ordinary authenticated user can access the user-management endpoints `/settings/users` and use them to enumerate all users and create a new administrator account. This happens because the route definitions do not enforce admin-only middleware, and the controller-level authorization check uses a broken boolean condition. As a result, any user with a valid web session cookie can reach functionality that should be restricted to administrators. Version 0.71.1 patches the issue.	8.8	More Details

CVE-2026-41445	KissFFT before commit 8a8e66e contains an integer overflow vulnerability in the kiss_fftndr_alloc() function in kiss_fftndr.c where the allocation size calculation dimOther*(dimReal+2)*sizeof(kiss_fft_scalar) overflows signed 32-bit integer arithmetic before being widened to size_t, causing malloc() to allocate an undersized buffer. Attackers can trigger heap buffer overflow by providing crafted dimensions that cause the multiplication to exceed INT_MAX, allowing writes beyond the allocated buffer region when kiss_fftndr() processes the data.	8.8	More Details
CVE-2023-3634	In products of the MSE6 product-family by Festo a remote authenticated, low privileged attacker could use functions of undocumented test mode which could lead to a complete loss of confidentiality, integrity and availability.	8.8	More Details
CVE-2026-32955	SD-330AC and AMC Manager provided by silex technology, Inc. contain a stack-based buffer overflow vulnerability in processing the redirect URLs. Arbitrary code may be executed on the device.	8.8	More Details
CVE-2026-34393	Weblate is a web based localization tool. In versions prior to 5.17, the user patching API endpoint didn't properly limit the scope of edits. This issue has been fixed in version 5.17.	8.8	More Details
CVE-2026-6249	Vvveb CMS 1.0.8 contains a remote code execution vulnerability in its media upload handler that allows authenticated attackers to execute arbitrary operating system commands by uploading a PHP webshell with a .phtml extension. Attackers can bypass the extension deny-list and upload malicious files to the publicly accessible media directory, then request the file over HTTP to achieve full server compromise.	8.8	More Details
CVE-2026-40349	Movary is a self hosted web app to track and rate a user's watched movies. Prior to version 0.71.1, an ordinary authenticated user can escalate their own account to administrator by sending `isAdmin=true` to `PUT /settings/users/{userId}` for their own user ID. The endpoint is intended to let a user edit their own profile, but it updates the sensitive `isAdmin` field without any admin-only authorization check. Version 0.71.1 patches the issue.	8.8	More Details
CVE-2026-29648	In OpenXiangShan NEMU, when Smstateen is enabled, clearing mstateen0.ENVCFG does not correctly restrict access to henvcfg and senvcfg. As a result, less-privileged code may read or write these CSRs without the required exception, potentially bypassing intended state-enable based isolation controls in virtualized or multi-privilege environments.	8.8	More Details
CVE-2026-40459	PAC4J is vulnerable to LDAP Injection in multiple methods. A low-privileged remote attacker can inject crafted LDAP syntax into ID-based search parameters, potentially resulting in unauthorized LDAP queries and arbitrary directory operations. This issue was fixed in PAC4J versions 4.5.10, 5.7.10 and 6.4.1	8.8	More Details
CVE-2026-6631	A vulnerability was determined in Tenda F451 1.0.0.7_cn_svn7958. Impacted is the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter of the component httpd. Executing a manipulation of the argument page can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-6630	A vulnerability was found in Tenda F451 1.0.0.7_cn_svn7958. This issue affects the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer of the component httpd. Performing a manipulation of the argument dips results in buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-31019	In the Website module of Dolibarr ERP & CRM 22.0.4 and below, the application uses blacklist-based filtering to restrict dangerous PHP functions related to system command execution. An authenticated user with permission to edit PHP content can bypass this filtering, resulting in full remote code execution with the ability to execute arbitrary operating system commands on the server.	8.8	More Details
CVE-2026-31018	In Dolibarr ERP & CRM <= 22.0.4, PHP code detection and editing permission enforcement in the Website module is not applied consistently to all input parameters, allowing an authenticated user restricted to HTML/JavaScript editing to inject PHP code through unprotected inputs during website page creation.	8.8	More Details
CVE-2026-3614	The AcyMailing plugin for WordPress is vulnerable to privilege escalation in all versions From 9.11.0 up to, and including, 10.8.1 due to a missing capability check on the `wp_ajax_acymailing_router` AJAX handler. This makes it possible for authenticated attackers, with Subscriber-level access and above, to access admin-only controllers (including configuration management), enable the autologin feature, create a malicious newsletter subscriber with an injected `cms_id` pointing to any WordPress user, and then use the autologin URL to authenticate as that user, including administrators.	8.8	More Details
CVE-2026-40352	FastGPT is an AI Agent building platform. In versions prior to 4.14.9.5, the password change endpoint is vulnerable to NoSQL injection. An authenticated attacker can bypass the "old password" verification by injecting MongoDB query operators. This allows an attacker who has gained a low-privileged session to change the password of their account (or others if combined with ID manipulation) without knowing the current one, leading to full account takeover and persistence. This issue has been fixed in version 4.14.9.5.	8.8	More Details
CVE-2026-41303	OpenClaw before 2026.3.28 contains an authorization bypass vulnerability in Discord text approval commands that allows non-approvers to resolve pending exec approvals. Attackers can send Discord text commands to bypass the channels.discord.execApprovals.approvers allowlist and approve pending host execution requests.	8.8	More Details
CVE-2026-1620	The Livemesh Addons for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 9.0. This is due to insufficient sanitization of the template name parameter in the `lae_get_template_part()` function, which uses an inadequate `str_replace()` approach that can be bypassed using recursive directory traversal patterns. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the attacker to include and execute local files via the widget's template parameter granted they can trick an administrator into performing an action or install Elementor.	8.8	More Details
CVE-2026-6581	A vulnerability was detected in H3C Magic B1 up to 100R004. Affected by this vulnerability is the function SetMobileAPInfoById of the file /goform/aspForm. Performing a manipulation of the argument param results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
	Neko is a a self-hosted virtual browser that runs in Docker and uses WebRTC In versions 3.0.0 through 3.0.10 and 3.1.0		

CVE-2026-39386	through 3.1.1, any authenticated user can immediately obtain full administrative control of the entire Neko instance (member management, room settings, broadcast control, session termination, etc.). This results in a complete compromise of the instance. The vulnerability has been patched in v3.0.11 and v3.1.2. If upgrading is not immediately possible, the following mitigations can reduce risk: Restrict access to trusted users only (avoid granting accounts to untrusted parties); ensure all user passwords are strong and only shared with trusted individuals; run the instance only when needed; avoid leaving it continuously exposed; place the instance behind authentication layers such as a reverse proxy with additional access controls; disable or restrict access to the /api/profile endpoint if feasible; and/or monitor for suspicious privilege changes or unexpected administrative actions. Note that these are temporary mitigations and do not fully eliminate the vulnerability. Upgrading is strongly recommended.	8.8	More Details
CVE-2026-40285	WeGIA is a web manager for charitable institutions. Versions prior to 3.6.10 contain a SQL injection vulnerability in dao/memorando/UsuarioDAO.php. The cpf_usuario POST parameter overwrites the session-stored user identity via extract($_REQUEST) in DespachoControle::verificarDespacho(), and the attacker-controlled value is then interpolated directly into a raw SQL query, allowing any authenticated user to query the database under an arbitrary identity. Version 3.6.10 fixes the issue.	8.8	More Details
CVE-2026-6632	A vulnerability was identified in Tenda F451 1.0.0.7_cn_svn7958. The affected element is the function fromSafeClientFilter of the file /goform/SafeClientFilter of the component httpd. The manipulation of the argument menufacturer/Go leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-6300	Use after free in CSS in Google Chrome prior to 147.0.7727.101 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-2026-6301	Type Confusion in Turbofan in Google Chrome prior to 147.0.7727.101 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-2026-6360	Use after free in FileSystem in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-40502	OpenHarness prior to commit dd1d235 contains a command injection vulnerability that allows remote gateway users with chat access to invoke sensitive administrative commands by exploiting insufficient distinction between local-only and remote-safe commands in the gateway handler. Attackers can execute administrative commands such as /permissions full_auto through remote chat sessions to change permission modes of a running OpenHarness instance without operator authorization.	8.8	More Details
CVE-2026-26944	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a missing authentication for critical function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. Exploitation requires an authenticated user to perform a specific action.	8.8	More Details
CVE-2026-34427	Vvveb prior to 1.0.8.1 contains a privilege escalation vulnerability in the admin user profile save endpoint that allows authenticated users to modify privileged fields on their own profile. Attackers can inject role_id=1 into profile save requests to escalate to Super Administrator privileges, enabling plugin upload functionality for remote code execution.	8.8	More Details
CVE-2026-40316	OWASP BLT is a QA testing and vulnerability disclosure platform that encompasses websites, apps, git repositories, and more. Versions prior to 2.1.1 contain an RCE vulnerability in the .github/workflows/regenerate-migrations.yml workflow. The workflow uses the pull_request_target trigger to run with full GITHUB_TOKEN write permissions, copies attacker-controlled files from untrusted pull requests into the trusted runner workspace via git show, and then executes python manage.py makemigrations, which imports Django model modules including attacker-controlled website/models.py at runtime. Any module-level Python code in the attacker's models.py is executed during import, enabling arbitrary code execution in the privileged CI environment with access to GITHUB_TOKEN and repository secrets. The attack is triggerable by any external contributor who can open a pull request, provided a maintainer applies the regenerate-migrations label, potentially leading to secret exfiltration, repository compromise, and supply chain attacks. A patch for this issue is expected to be released in version 2.1.1.	8.8	More Details
CVE-2026-6560	A security vulnerability has been detected in H3C Magic B0 up to 100R002. This vulnerability affects the function Edit_BasicSSID of the file /goform/aspForm. Such manipulation of the argument param leads to buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-6819	HKUDS OpenHarness prior to PR #156 remediation exposes plugin lifecycle commands including /plugin install, /plugin enable, /plugin disable, and /reload-plugins to remote senders by default. Attackers who gain access through the channel layer can remotely manage plugin trust and activation state, enabling unauthorized plugin installation and activation on the system.	8.8	More Details
CVE-2026-40261	Composer is a dependency manager for PHP. Versions 1.0 through 2.2.26 and 2.3 through 2.9.5 contain a command injection vulnerability in the Perforce::syncCodeBase() method, which appends the $sourceReference parameter to a shell command without proper escaping, and additionally in the Perforce::generateP4Command() method as in GHSA-wg36-wvj6-r67p / CVE-2026-40176, which interpolates user-supplied Perforce connection parameters (port, user, client) from the source url field without proper escaping. An attacker can inject arbitrary commands through crafted source reference or source url values containing shell metacharacters, even if Perforce is not installed. Unlike CVE-2026-40176, the source reference and url are provided as part of package metadata, meaning any compromised or malicious Composer repository can serve package metadata declaring perforce as a source type with malicious values. This vulnerability is exploitable when installing or updating dependencies from source, including the default behavior when installing dev-prefixed versions. This issue has been fixed in Composer 2.2.27 (2.2 LTS) and 2.9.6 (mainline). If developers are unable to immediately update, they can avoid installing dependencies from source by using --prefer-dist or the preferred-install: dist config setting, and only use trusted Composer repositories as a workaround.	8.8	More Details

CVE-2026-30898	An example of BashOperator in Airflow documentation suggested a way of passing dag_run.conf in the way that could cause unsanitized user input to be used to escalate privileges of UI user to allow execute code on worker. Users should review if any of their own DAGs have adopted this incorrect advice.	8.8	More Details
CVE-2026-6518	The CMP – Coming Soon & Maintenance Plugin by NiteoThemes plugin for WordPress is vulnerable to arbitrary file upload and remote code execution in all versions up to, and including, 4.1.16 via the `cmp_theme_update_install` AJAX action. This is due to the function only checking for the `publish_pages` capability (available to Editors and above) instead of `manage_options` (Administrators only), combined with a lack of proper validation on the user-supplied file URL and no verification of the downloaded file's content before extraction. This makes it possible for authenticated attackers, with Administrator-level access and above, to force the server to download and extract a malicious ZIP file from a remote attacker-controlled URL into a web-accessible directory (`wp-content/plugins/cmp-premium-themes/`), resulting in remote code execution. Due to the lack of a nonce for Editors, they are unable to exploit this vulnerability.	8.8	More Details
CVE-2026-6363	Type Confusion in V8 in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-6359	Use after free in Video in Google Chrome on Windows prior to 147.0.7727.101 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-6302	Use after free in Video in Google Chrome prior to 147.0.7727.101 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-2026-6358	Use after free in XR in Google Chrome on Android prior to 147.0.7727.101 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-6348	WinMatrix agent developed by Simopro Technology has a Missing Authentication vulnerability, allowing authenticated local attackers to execute arbitrary code with SYSTEM privileges on the local machine as well as on all hosts within the environment where the agent is installed.	8.8	More Details
CVE-2026-6318	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 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-2026-6317	Use after free in Cast in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-6316	Use after free in Forms in Google Chrome prior to 147.0.7727.101 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-2026-6315	Use after free in Permissions in Google Chrome on Android prior to 147.0.7727.101 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-2026-6307	Type Confusion in Turbofan in Google Chrome prior to 147.0.7727.101 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-2026-6306	Heap buffer overflow in PDFium in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-6305	Heap buffer overflow in PDFium in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-6303	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 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-2026-3464	The WP Customer Area plugin for WordPress is vulnerable to arbitrary file read and deletion due to insufficient file path validation in the 'ajax_attach_file' function in all versions up to, and including, 8.3.4. This makes it possible for authenticated attackers with a role that an administrator grants access to (e.g., Subscriber) to to read the contents of arbitrary files on the server, which can contain sensitive information, or delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details
CVE-2026-6563	A vulnerability has been found in H3C Magic B1 up to 100R004. The affected element is the function SetAPWifiorLedInfoById of the file /goform/aspForm. The manipulation of the argument param leads to buffer overflow. 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.	8.8	More Details
CVE-2026-33121	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the API datasource saving process. The deTableName field from the Base64-encoded datasource configuration is used to construct a DDL statement via simple string replacement without any sanitization or escaping of the table name. An authenticated attacker can inject arbitrary SQL commands by crafting a deTableName that breaks out of identifier quoting, enabling error-based SQL injection that can extract database information such as the MySQL version. This issue has	8.8	More Details

	been fixed in version 2.10.21.		
CVE-2026-33084	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the sort parameter of the /de2api/datasetData/enumValueObj endpoint. The DatasetDataManage service layer directly transfers the user-supplied sort value to the sorting metadata DTO, which is passed to Order2SQLObj where it is incorporated into the SQL ORDER BY clause without any whitelist validation, and then executed via CalciteProvider. An authenticated attacker can inject arbitrary SQL commands through the sort parameter, enabling time-based blind SQL injection. This issue has been fixed in version 2.10.21.	8.8	More Details
CVE-2026-33083	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the orderDirection parameter used in dataset-related endpoints including /de2api/datasetData/enumValueDs and /de2api/datasetTree/exportDataset. The Order2SQLObj class directly assigns the raw user-supplied orderDirection value into the SQL query without any validation or whitelist enforcement, and the value is rendered into the ORDER BY clause via StringTemplate before being executed against the database. An authenticated attacker can inject arbitrary SQL commands through the sorting direction field, enabling time-based blind data extraction and denial of service. This issue has been fixed in version 2.10.21.	8.8	More Details
CVE-2026-5617	The Login as User plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the handle_return_to_admin() function trusting a client-controlled cookie (oclaup_original_admin) to determine which user to authenticate as, without any server-side verification that the cookie value was legitimately set during an admin-initiated user switch. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their privileges to administrator by setting the oclaup_original_admin cookie to an administrator's user ID and triggering the "Return to Admin" functionality.	8.8	More Details
CVE-2026-32107	xrdp is an open source RDP server. In versions through 0.10.5, the session execution component did not properly handle an error during the privilege drop process. This improper privilege management could allow an authenticated local attacker to escalate privileges to root and execute arbitrary code on the system. An additional exploit would be needed to facilitate this. This issue has been fixed in version 0.10.6.	8.8	More Details
CVE-2026-6769	Privilege escalation in the Debugger component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	8.8	More Details
CVE-2026-40066	Anviz CX2 Lite and CX7 are vulnerable to unverified update packages that can be uploaded. The device unpacks and executes a script resulting in unauthenticated remote code execution.	8.8	More Details
CVE-2026-33207	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the /datasource/getTableField endpoint. The getTableFiledSql method in CalciteProvider.java incorporates the tableName parameter directly into SQL query strings using String.format without parameterization or sanitization. Although DatasourceServer.java validates that the table name exists in the datasource, an attacker can bypass this by first registering an API datasource with a malicious deTableName, which is then returned by getTables and passes the validation check. An authenticated attacker can execute arbitrary SQL commands, enabling error-based extraction of sensitive database information. This issue has been fixed in version 2.10.21.	8.8	More Details
CVE-2026-35682	Anviz CX2 Lite is vulnerable to an authenticated command injection via a filename parameter that enables arbitrary command execution (e.g., starting telnetd), resulting in root-level access.	8.8	More Details
CVE-2026-40900	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the /de2api/datasetData/previewSql endpoint. The user-supplied SQL is wrapped in a subquery without validation that the input is a single SELECT statement. Combined with the JDBC blocklist bypass that allows enabling allowMultiQueries=true, an attacker can break out of the subquery and execute arbitrary stacked SQL statements, including UPDATE and other write operations, against the connected database. An authenticated attacker with access to valid datasource credentials can achieve full read and write access to the underlying database. This issue has been fixed in version 2.10.21.	8.8	More Details
CVE-2026-40611	Let's Encrypt client and ACME library written in Go (Lego). Prior to 4.34.0, the webroot HTTP-01 challenge provider in lego is vulnerable to arbitrary file write and deletion via path traversal. A malicious ACME server can supply a crafted challenge token containing ../ sequences, causing lego to write attacker-influenced content to any path writable by the lego process. This vulnerability is fixed in 4.34.0.	8.8	More Details
CVE-2025-14868	The Career Section plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Path Traversal and Arbitrary File Deletion in all versions up to, and including, 1.6. This is due to missing nonce validation and insufficient file path validation on the delete action in the 'appform_options_page_html' function. This makes it possible for unauthenticated attackers to delete arbitrary files on the server via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2026-5967	ThreatSonar Anti-Ransomware developed by TeamT5 has an Privilege Escalation vulnerability. Authenticated remote attackers with shell access can inject OS commands and execute them with root privileges.	8.8	More Details
CVE-2026-6761	Privilege escalation in the Networking component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	8.8	More Details
CVE-2026-6750	Privilege escalation in the Graphics: WebRender component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	8.8	More Details
	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Core). Supported versions that are		

CVE-2026-34291	affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. While the vulnerability is in Oracle HTTP Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HTTP Server accessible data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	8.7	More Details
CVE-2026-40909	WWBN AVideo is an open source video platform. In versions 29.0 and prior, the locale save endpoint (`locale/save.php`) constructs a file path by directly concatenating `$_POST['flag']` into the path at line 30 without any sanitization. The `$_POST['code']` parameter is then written verbatim to that path via `fwrite()` at line 40. An admin attacker (or any user who can CSRF an admin, since no CSRF token is checked and cookies use `SameSite=None`) can traverse out of the `locale/` directory and write arbitrary `.php` files to any writable location on the filesystem, achieving Remote Code Execution. Commit 57f89ffbc27d37c9d9dd727212334846e78ac21a fixes the issue.	8.7	More Details
CVE-2026-40262	Note Mark is an open-source note-taking application. In versions 0.19.1 and prior, the asset delivery handler serves uploaded files inline and relies on magic-byte detection for content type, which does not identify text-based formats such as HTML, SVG, or XHTML. These files are served with an empty Content-Type, no X-Content-Type-Options: nosniff header, and inline disposition, allowing browsers to sniff and render active content. An authenticated user can upload an HTML or SVG file containing JavaScript as a note asset, and when a victim navigates to the asset URL, the script executes under the application's origin with access to the victim's authenticated session and API actions. This issue has been fixed in version 0.19.2.	8.7	More Details
CVE-2026-35569	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain a stored cross-site scripting vulnerability in SEO-related fields (SEO Title and Meta Description), where user-controlled input is rendered without proper output encoding into HTML contexts including <title> tags, <meta> attributes, and JSON-LD structured data. An attacker can inject a payload such as "></title><script>alert(1)</script> to break out of the intended HTML context and execute arbitrary JavaScript in the browser of any authenticated user who views the affected page. This can be leveraged to perform authenticated API requests, access sensitive data such as usernames, email addresses, and roles via internal APIs, and exfiltrate it to an attacker-controlled server. This issue has been fixed in version 4.29.0.	8.7	More Details
CVE-2026-30995	Slah CMS v1.5.0 and below was discovered to contain a SQL injection vulnerability via the id parameter in the vereador_ver.php endpoint.	8.6	More Details
CVE-2026-41294	OpenClaw before 2026.3.28 loads the current working directory .env file before trusted state-dir configuration, allowing environment variable injection. Attackers can place a malicious .env file in a repository or workspace to override runtime configuration and security-sensitive environment settings during OpenClaw startup.	8.6	More Details
CVE-2026-22734	Cloud Foundry UUA is vulnerable to a bypass that allows an attacker to obtain a token for any user and gain access to UAA-protected systems. This vulnerability exists when SAML 2.0 bearer assertions are enabled for a client, as the UAA accepts SAML 2.0 bearer assertions that are neither signed nor encrypted. This issue affects UUA from v77.30.0 to v78.7.0 (inclusive) and it affects CF Deployment from v48.7.0 to v54.14.0 (inclusive).	8.6	More Details
CVE-2026-41055	WWBN AVideo is an open source video platform. In versions 29.0 and below, an incomplete SSRF fix in AVideo's LiveLinks proxy adds `isSSRFSafeURL()` validation but leaves DNS TOCTOU vulnerabilities where DNS rebinding between validation and the actual HTTP request redirects traffic to internal endpoints. Commit 8d8fc0cadb425835b4861036d589abcea4d78ee8 contains an updated fix.	8.6	More Details
CVE-2026-30617	LangChain-ChatChat 0.3.1 contains a remote code execution vulnerability in its MCP STDIO server configuration and execution handling. A remote attacker can access the publicly exposed MCP management interface and configure an MCP STDIO server with attacker-controlled commands and arguments. When the MCP server is started and MCP is enabled for agent execution, subsequent agent activity triggers execution of arbitrary commands on the server. Successful exploitation allows arbitrary command execution within the context of the LangChain-ChatChat service.	8.6	More Details
CVE-2026-30624	Agent Zero 0.9.8 contains a remote code execution vulnerability in its External MCP Servers configuration feature. The application allows users to define MCP servers using a JSON configuration containing arbitrary command and args values. These values are executed by the application when the configuration is applied without sufficient validation or restriction. An attacker may supply a malicious MCP configuration to execute arbitrary operating system commands, potentially resulting in remote code execution with the privileges of the Agent Zero process.	8.6	More Details
CVE-2026-40318	SiYuan is an open-source personal knowledge management system. In versions 3.6.3 and prior, the /api/av/removeUnusedAttributeView endpoint constructs a filesystem path using the user-controlled id parameter without validation or path boundary enforcement. An attacker can inject path traversal sequences such as ../ into the id value to escape the intended directory and delete arbitrary .json files on the server, including global configuration files and workspace metadata. This issue has been fixed in version 3.6.4.	8.5	More Details
CVE-2026-21997	Vulnerability in the Oracle Life Sciences Empirica Signal product of Oracle Life Science Applications (component: Common Core). Supported versions that are affected are 9.2.1-9.2.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Life Sciences Empirica Signal. While the vulnerability is in Oracle Life Sciences Empirica Signal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Life Sciences Empirica Signal accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Empirica Signal accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N).	8.5	More Details
CVE-	FreeScout is a free self-hosted help desk and shared mailbox. Versions prior to 1.8.213 have a stored cross-site scripting (XSS) vulnerability in the mailbox signature feature. The sanitization function `Helper::stripDangerousTags()` (`app/Misc/Helper.php:568`) uses an incomplete blocklist of only four HTML tags (`script`, `form`, `iframe`, `object`) and does not remove event handler attributes. When a mailbox signature is saved via `MailboxesController::updateSave()` (`app/Http/Controllers/MailboxesController.php:267`), HTML elements such as `<img>`, `<svg>`, and `<details>` with event handler attributes like `onerror` and `onload` pass through sanitization unchanged and are stored in the database. The		

2026-40568	signature is then rendered as raw HTML via the Blade `{!! !!}` tag in `editor_bottom_toolbar.blade.php:6` and re-inserted into the visible DOM by jQuery `.html()` at `main.js:1789-1790`, triggering the injected event handlers. Any authenticated user with the `ACCESS_PERM_SIGNATURE` (`sig`) permission on a mailbox -- a delegatable, non-admin permission -- can inject arbitrary HTML and JavaScript into the mailbox signature. The payload fires automatically, with no victim interaction, whenever any agent or administrator opens any conversation in the affected mailbox. This enables session hijacking (under CSP bypass conditions such as IE11 or module-weakened CSP), phishing overlays that work in all browsers regardless of CSP, and chaining to admin-level actions including email exfiltration via mass assignment and self-propagating worm behavior across all mailboxes. Version 1.8.213 fixes the issue.	8.5	More Details
CVE-2026-40744	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Beaver Builder Beaver Builder beaver-builder-lite-version allows Blind SQL Injection.This issue affects Beaver Builder: from n/a through <= 2.10.1.2.	8.5	More Details
CVE-2026-23853	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a use of weak credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to the system.	8.4	More Details
CVE-2026-4857	IdentityIQ 8.5, all IdentityIQ 8.5 patch levels prior to 8.5p2, IdentityIQ 8.4, and all IdentityIQ 8.4 patch levels prior to 8.4p4 allow authenticated users assigned the Debug Pages Read Only capability or any custom capability with the ViewAccessDebugPage SPRight to incorrectly create new IdentityIQ objects. Until a remediating security fix or patches containing this security fix are installed, the Debug Pages Read Only capability and any custom capabilities that contain the ViewAccessDebugPage SPRight should be unassigned from all identities and workgroups.	8.4	More Details
CVE-2026-3517	OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an authenticated attacker with “Geo Administration” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in the 'addcountry' command	8.4	More Details
CVE-2026-3518	OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an authenticated attacker with “All” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in the 'killsession' command	8.4	More Details
CVE-2026-3519	OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an authenticated attacker with “VS Administration” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in the 'aclcontrol' command	8.4	More Details
CVE-2026-4048	OS Command Injection Remote Code Execution Vulnerability in UI in Progress ADC Products allows an authenticated attacker with “All” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in a custom WAF rule file during the file upload process.	8.4	More Details
CVE-2026-40706	In NTFS-3G 2022.10.3 before 2026.2.25, a heap buffer overflow exists in ntfs_build_permissions_posix() in acls.c that allows an attacker to corrupt heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered on the READ path (stat, readdir, open) when processing a security descriptor with multiple ACCESS_DENIED ACEs containing WRITE_OWNER from distinct group SIDs.	8.4	More Details
CVE-2026-35570	OpenClaude is an open-source coding-agent command line interface for cloud and local model providers. Versions prior to 0.5.1 have a logic flaw in `bashToolHasPermission()` inside `src/tools/BashTool/bashPermissions.ts`. When the sandbox auto-allow feature is active and no explicit deny rule is configured, the function returns an `allow` result immediately — before the path constraint filter (`checkPathConstraints`) is ever evaluated. This allows commands containing path traversal sequences (e.g., `../../../../../etc/passwd`) to bypass directory restrictions entirely. Version 0.5.1 contains a patch for the issue.	8.4	More Details
CVE-2024-53412	Command injection in the connect function in NietThijmen ShoppingCart 0.0.2 allows an attacker to execute arbitrary shell commands and achieve remote code execution via injection of malicious payloads into the Port field	8.4	More Details
CVE-2026-40931	Compressing is a compressing and uncompressing lib for node. Prior to 2.1.1 and 1.10.5, the patch for CVE-2026-24884 relies on a purely logical string validation within the isPathWithinParent utility. This check verifies if a resolved path string starts with the destination directory string but fails to account for the actual filesystem state. By exploiting this "Logical vs. Physical" divergence, an attacker can bypass the security check using a Directory Poisoning technique (pre-existing symbolic links). This vulnerability is fixed in 2.1.1 and 1.10.5.	8.4	More Details
CVE-2026-6304	Use after free in Graphite in Google Chrome prior to 147.0.7727.101 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-2026-6309	Use after free in Viz in Google Chrome prior to 147.0.7727.101 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-2026-6310	Use after free in Dawn in Google Chrome prior to 147.0.7727.101 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-2026-6297	Use after free in Proxy in Google Chrome prior to 147.0.7727.101 allowed an attacker in a privileged network position to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-6311	Uninitialized Use in Accessibility in Google Chrome on Windows prior to 147.0.7727.101 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-2026-6314	Out of bounds write in GPU in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who had compromised the GPU process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-30461	Daylight Studio FuelCMS v1.5.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the /controllers/Installer.php and the function add_git_submodule.	8.3	More Details
CVE-2026-6442	Improper validation of bash commands in Snowflake Cortex Code CLI versions prior to 1.0.25 allowed subsequent commands to execute outside the sandbox. An attacker could exploit this by embedding specially crafted commands in untrusted content, such as a malicious repository, causing the CLI agent to execute arbitrary code on the local device without user consent. Exploitation is non-deterministic and model-dependent. The fix is automatically applied upon relaunch with no user action required.	8.3	More Details
CVE-2026-39884	mcp-server-kubernetes is a Model Context Protocol server for Kubernetes cluster management. Versions 3.4.0 and prior contain an argument injection vulnerability in the port_forward tool in src/tools/port_forward.ts, where a kubectl command is constructed via string concatenation with user-controlled input and then naively split on spaces before being passed to spawn(). Unlike all other tools in the codebase which correctly use array-based argument passing with execFileSync(), port_forward treats every space in user-controlled fields (namespace, resourceType, resourceName, localPort, targetPort) as an argument boundary, allowing an attacker to inject arbitrary kubectl flags. This enables exposure of internal Kubernetes services to the network by injecting --address=0.0.0.0, cross-namespace targeting by injecting additional -n flags, and indirect exploitation via prompt injection against AI agents connected to the MCP server. This issue has been fixed in version 3.5.0.	8.3	More Details
CVE-2026-40516	OpenHarness before commit bd4df81 contains a server-side request forgery vulnerability in the web_fetch and web_search tools that allows attackers to access private and localhost HTTP services by manipulating tool parameters without proper validation of target addresses. Attackers can influence an agent session to invoke these tools against loopback, RFC1918, link-local, or other non-public addresses to read response bodies from local development services, cloud metadata endpoints, admin panels, or other private HTTP services reachable from the victim host.	8.3	More Details
CVE-2026-40925	WWBN AVideo is an open source video platform. In versions 29.0 and prior, `objects/configurationUpdate.json.php` (also routed via `/updateConfig`) persists dozens of global site settings from `$_POST` but protects the endpoint only with `User::isAdmin()`. It does not call `forbidIfIsUntrustedRequest()`, does not verify a `globalToken`, and does not validate the Origin/Referer header. Because AVideo intentionally sets `session.cookie_samesite=None` to support cross-origin iframe embedding, a logged-in administrator who visits an attacker-controlled page will have the browser auto-submit a cross-origin POST that rewrites the site's encoder URL, SMTP credentials, site `<head>` HTML, logo, favicon, contact email, and more in a single request. Commit f9492f5e6123dff0292d5bb3164fde7665dc36b4 contains a fix.	8.3	More Details
CVE-2026-39110	SQL Injection vulnerability in Apartment Visitors Management System Apartment Visitors Management System V1.1 in the contactno parameter of the forgot password page (forgot-password.php). This allows an unauthenticated attacker to manipulate backend SQL queries during authentication and retrieve sensitive database contents.	8.2	More Details
CVE-2026-28224	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, when the server receives an op_crypt_key_callback packet without prior authentication, the port_server_crypt_callback handler is not initialized, resulting in a null pointer dereference and server crash. An unauthenticated attacker who knows only the server's IP and port can exploit this to crash the server. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	8.2	More Details
CVE-2026-6823	HKUDS OpenHarness prior to PR #147 remediation contains an insecure default configuration vulnerability where remote channels inherit allow_from = ["*"] permitting arbitrary remote senders to pass admission checks. Attackers who can reach the configured channel can bypass access controls and reach host-backed agent runtimes, potentially leading to unauthorized file disclosure and read access through default-enabled read-only tools.	8.2	More Details
CVE-2026-34632	Adobe Photoshop Installer was affected by an Uncontrolled Search Path Element vulnerability that could have resulted in arbitrary code execution in the context of the current user. A low-privileged local attacker could have exploited this vulnerability by manipulating the search path used by the application to locate critical resources, potentially causing unauthorized code execution. Exploitation of this issue required user interaction in that a user had to be running the installer.	8.2	More Details
CVE-2026-40193	maddy is a composable, all-in-one mail server. Versions prior to 0.9.3 contain an LDAP injection vulnerability in the auth.ldap module where user-supplied usernames are interpolated into LDAP search filters and DN strings via strings.ReplaceAll() without any LDAP filter escaping, despite the go-ldap/ldap/v3 library's ldap.EscapeFilter() function being available in the same import. This affects three code paths: the Lookup() filter, the AuthPlain() DN template, and the AuthPlain() filter. An attacker with network access to the SMTP submission or IMAP interface can inject arbitrary LDAP filter expressions through the username field in AUTH PLAIN or LOGIN commands. This enables identity spoofing by manipulating filter results to authenticate as another user, LDAP directory enumeration via wildcard filters, and blind extraction of LDAP attribute values using authentication responses as a boolean oracle or via timing side-channels between the two distinct failure paths. This issue has been fixed in version 0.9.3.	8.2	More Details
CVE-2026-3324	Zohocorp ManageEngine Log360 versions 13000 through 13013 are vulnerable to authentication bypass on certain actions due to improper filter configuration.	8.2	More Details
CVE-2026-24189	NVIDIA CUDA-Q contains a vulnerability in an endpoint, where an unauthenticated attacker could cause an out-of-bounds read by sending a maliciously crafted request. A successful exploit of this vulnerability might lead to denial of service and information disclosure.	8.2	More Details
CVE-2026-27890	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, when processing CNCT_specific_data segments during authentication, the server assumes segments arrive in strictly ascending order. If segments arrive out of order, the Array class's grow() method computes a negative size value, causing a SIGSEGV crash. An unauthenticated attacker who knows only the server's IP and port can exploit this to crash the server. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	8.2	More Details

CVE-2026-41296	OpenClaw before 2026.3.31 contains a time-of-check-time-of-use race condition in the remote filesystem bridge readFile function that allows sandbox escape. Attackers can exploit the separate path validation and file read operations to bypass sandbox restrictions and read arbitrary files.	8.2	More Details
CVE-2026-40104	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Versions 1.8-rc-1, 17.0.0-rc-1 and 17.5.0-rc-1 and prior include a resource exhaustion vulnerability in REST API endpoints such as /xwiki/rest/wikis/xwiki/spaces/AnnotationCode/pages/AnnotationConfig/objects/AnnotationCode.AnnotationConfig/0/properties, which list all available pages as part of the metadata for database list properties without applying query limits. On large wikis, this can exhaust available server resources. This issue has been patched in versions 16.10.16, 17.4.8 and 17.10.1.	8.2	More Details
CVE-2026-5966	ThreatSonar Anti-Ransomware developed by TeamT5 has an Arbitrary File Deletion vulnerability. Authenticated remote attackers with web access can exploit Path Traversal to delete arbitrary files on the system.	8.1	More Details
CVE-2026-6832	Hermes WebUI contains an arbitrary file deletion vulnerability in the /api/session/delete endpoint that allows authenticated attackers to delete files outside the session directory by supplying an absolute path or path traversal payload in the session_id parameter. Attackers can exploit unvalidated session identifiers to construct paths that bypass the SESSION_DIR boundary and delete writable JSON files on the host system.	8.1	More Details
CVE-2026-6248	The wpForo Forum plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to and including 3.0.5. This is due to two compounding flaws: the Members::update() method does not validate or restrict the value of file-type custom profile fields, allowing authenticated users to store an arbitrary path instead of a legitimate upload path; and the wpforo_fix_upload_dir() sanitization function in ucf_file_delete() only remaps paths that match the expected pattern, and it is passed directly to the unlink() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Note: The vulnerability requires a file custom field, which requires the wpForo - User Custom Fields addon plugin.	8.1	More Details
CVE-2026-41058	WWBN AVideo is an open source video platform. In versions 29.0 and below, the incomplete fix for AVideo's CloneSite `deleteDump` parameter does not apply path traversal filtering, allowing `unlink()` of arbitrary files via `../../` sequences in the GET parameter. Commit 3c729717c26f160014a5c86b0b6accdbd613e7b2 contains an updated fix.	8.1	More Details
CVE-2026-40764	Cross-Site Request Forgery (CSRF) vulnerability in Syed Balkhi Contact Form by WPForms wpforms-lite allows Cross Site Request Forgery.This issue affects Contact Form by WPForms: from n/a through <= 1.10.0.2.	8.1	More Details
CVE-2026-40434	Anviz CrossChex Standard lacks source verification in the client/server channel, enabling TCP packet injection by an attacker on the same network to alter or disrupt application traffic.	8.1	More Details
CVE-2026-25524	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 version 20.17.0, PHP functions such as `getimagesize()`, `file_exists()`, and `is_readable()` can trigger deserialization when processing `phar://` stream wrapper paths. OpenMage LTS uses these functions with potentially controllable file paths during image validation and media handling. An attacker who can upload a malicious phar file (disguised as an image) and trigger one of these functions with a `phar://` path can achieve arbitrary code execution. Version 20.17.0 patches the issue.	8.1	More Details
CVE-2026-40784	Authorization Bypass Through User-Controlled Key vulnerability in Mahmudul Hasan Arif FluentBoards fluent-boards allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FluentBoards: from n/a through <= 1.91.2.	8.1	More Details
CVE-2025-54550	The example example_xcom that was included in airflow documentation implemented unsafe pattern of reading value from xcom in the way that could be exploited to allow UI user who had access to modify XComs to perform arbitrary execution of code on the worker. Since the UI users are already highly trusted, this is a Low severity vulnerability. It does not affect Airflow release - example_dags are not supposed to be enabled in production environment, however users following the example could replicate the bad pattern. Documentation of Airflow 3.2.0 contains version of the example with improved resiliance for that case. Users who followed that pattern are advised to adjust their implementations accordingly.	8.1	More Details
CVE-2025-40897	An access control vulnerability was discovered in the Threat Intelligence functionality due to a specific access restriction not being properly enforced for users with view-only privileges. An authenticated user with view-only privileges for the Threat Intelligence functionality can perform administrative actions on it, altering the rules configuration, and/or affecting their availability.	8.1	More Details
CVE-2026-41056	WWBN AVideo is an open source video platform. In versions 29.0 and below, the `allowOrigin($allowAll=true)` function in `objects/functions.php` reflects any arbitrary `Origin` header back in `Access-Control-Allow-Origin` along with `Access-Control-Allow-Credentials: true`. This function is called by both `plugin/API/get.json.php` and `plugin/API/set.json.php` — the primary API endpoints that handle user data retrieval, authentication, livestream credentials, and state-changing operations. Combined with the application's `SameSite=None` session cookie policy, any website can make credentialed cross-origin requests and read authenticated API responses, enabling theft of user PII, livestream keys, and performing state changes on behalf of the victim. Commit caf705f38eae0ccfac4c3af1587781355d24495e contains a fix.	8.1	More Details
CVE-2026-40868	Kyverno is a policy engine designed for cloud native platform engineering teams. Prior to 1.16.4, kyverno's apiCall servicecall helper implicitly injects Authorization: Bearer ... using the kyverno controller serviceaccount token when a policy does not explicitly set an Authorization header. Because context.apiCall.service.url is policy-controlled, this can send the kyverno serviceaccount token to an attacker-controlled endpoint (confused deputy). Namespaced policies are blocked from servicecall usage by the namespaced urlPath gate in pkg/engine/apicall/apiCall.go, so this report is scoped to ClusterPolicy and global context usage. This vulnerability is fixed in 1.16.4.	8.1	More Details
CVE-2026-	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the family record deletion endpoint (SelectDelete.php) performs permanent, irreversible deletion of family records and all associated data via a plain GET request with no CSRF token validation. An attacker can craft a malicious page that, when visited by an authenticated administrator,	8.1	More

40581	silently triggers deletion of targeted family records including associated notes, pledges, persons, and property data without any user interaction. This issue has been fixed in version 7.2.0.		Details
CVE-2026-40259	SiYuan is an open-source personal knowledge management system. In versions 3.6.3 and below, the /api/av/removeUnusedAttributeView endpoint is protected only by generic authentication that accepts publish-service RoleReader tokens. The handler passes a caller-controlled id directly to a model function that unconditionally deletes the corresponding attribute view file from the workspace without verifying that the caller has write privileges or that the target attribute view is actually unused. An authenticated publish-service reader can permanently delete arbitrary attribute view definitions by extracting publicly exposed data-av-id values from published content, causing breakage of database views and workspace rendering until manually restored. This issue has been fixed in version 3.6.4.	8.1	More Details
CVE-2026-5478	The Everest Forms plugin for WordPress is vulnerable to Arbitrary File Read and Deletion in all versions up to, and including, 3.4.4. This is due to the plugin trusting attacker-controlled old_files data from public form submissions as legitimate server-side upload state, and converting attacker-supplied URLs into local filesystem paths using regex-based string replacement without canonicalization or directory boundary enforcement. This makes it possible for unauthenticated attackers to read arbitrary local files (e.g., wp-config.php) by injecting path-traversal payloads into the old_files upload field parameter, which are then attached to notification emails. The same path resolution is also used in the post-email cleanup routine, which calls unlink() on the resolved path, resulting in the targeted file being deleted after being attached. This can lead to full site compromise through disclosure of database credentials and authentication salts from wp-config.php, and denial of service through deletion of critical files. Prerequisite: The form must contain a file-upload or image-upload field, and disable storing entry information.	8.1	More Details
CVE-2026-41113	sagredo qmail before 2026.04.07 allows tls_quit remote code execution because of popen in notlshosts_auto in qmail-remote.c.	8.1	More Details
CVE-2026-40196	HomeBox is a home inventory and organization system. Versions prior to 0.25.0 contain a vulnerability where the defaultGroup ID remained permanently assigned to a user after being invited to a group, even after their access to that group was revoked. While the web interface correctly enforced the access revocation and prevented the user from viewing or modifying the group's contents, the API did not. Because the original group ID persisted as the user's defaultGroup, and this value was not properly validated when the X-Tenant header was omitted, the user could still perform full CRUD operations on the group's collections through the API, bypassing the intended access controls. This issue has been fixed in version 0.25.0.	8.1	More Details
CVE-2026-5718	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file upload in versions up to, and including, 1.3.9.6. This is due to insufficient file type validation that occurs when custom blacklist types are configured, which replaces the default dangerous extension denylist instead of merging with it, and the wpcf7_antiscript_file_name() sanitization function being bypassed for filenames containing non-ASCII characters. This makes it possible for unauthenticated attackers to upload arbitrary files, such as PHP files, to the server, which can be leveraged to achieve remote code execution.	8.1	More Details
CVE-2026-34309	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2026-40905	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.4, a password reset poisoning vulnerability was identified in the application due to improper trust of user-controlled HTTP headers. The application uses the X-Forwarded-Host header when generating password reset URLs. By manipulating this header during a password reset request, an attacker can inject an attacker-controlled domain into the reset link sent via email. As a result, the victim receives a password reset email containing a malicious link pointing to an attacker-controlled domain. When the victim clicks the link, the password reset token is transmitted to the attacker-controlled server. An attacker can capture this token and use it to reset the victim’s password, leading to full account takeover. This vulnerability is fixed in 2.5.4.	8.1	More Details
CVE-2026-40960	Luanti 5 before 5.15.2 sometimes allows unintended access to an insecure environment. If at least one mod is listed as secure.trusted_mods or secure.http_mods, then a crafted mod can intercept the request for the insecure environment or HTTP API, and also receive access to it.	8.1	More Details
CVE-2026-40588	blueprintUE is a tool to help Unreal Engine developers. Prior to 4.2.0, the password change form at /profile/{slug}/edit/ does not include a current_password field and does not verify the user's existing password before accepting a new one. Any attacker who obtains a valid authenticated session — through XSS exploitation, session sidejacking over HTTP, physical access to a logged-in browser, or a stolen "remember me" cookie — can immediately change the account password without knowing the original credential, resulting in permanent account takeover. This vulnerability is fixed in 4.2.0.	8.1	More Details
CVE-2026-3605	An authenticated user with access to a kvv2 path through a policy containing a glob may be able to delete secrets they were not authorized to read or write, resulting in denial-of-service. This vulnerability did not allow a malicious user to delete secrets across namespaces, nor read any secret data. Fxed in Vault Community Edition 2.0.0 and Vault Enterprise 2.0.0, 1.21.5, 1.20.10, and 1.19.16.	8.1	More Details
CVE-2026-40497	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, FreeScout's `Helper::stripDangerousTags()` removes `<script>`, `<form>`, `<iframe>`, `<object>` but does NOT strip `<style>` tags. The mailbox signature field is saved via POST /mailbox/settings/{id} and later rendered unescaped via `{!! $conversation->getSignatureProcessed([], true) !!}` in conversation views. CSP allows `style-src * 'self' 'unsafe-inline'`, so injected inline styles execute freely. An attacker with access to mailbox settings (admin or agent with mailbox permission) can inject CSS attribute selectors to exfiltrate the CSRF token of any agent/admin who views a conversation in that mailbox. With the CSRF token, the attacker can perform any state-changing action as the victim (create admin accounts, change email/password, etc.) — privilege escalation from agent to admin. This is the result of an incomplete fix of GHSA-jqjf-f566-485j. That advisory reported XSS via mailbox signature. The fix applied `Helper::stripDangerousTags()` to the signature before saving. However, `stripDangerousTags()` only removes `script`, `form`, `iframe`, and `object` tags — it does NOT strip `<style>` tags, leaving	8.1	More Details

	CSS injection possible. Version 1.8.213 contains an updated fix.		
CVE-2026-5785	Zohocorp ManageEngine PAM360 versions before 8531 and ManageEngine Password Manager Pro versions from 8600 to 13230 are vulnerable to Authenticated SQL injection in the query report module.	8.1	More Details
CVE-2026-6290	Velociraptor versions prior to 0.76.3 contain a vulnerability in the query() plugin which allows access to all orgs with the user's current ACL token. This allows an authenticated GUI user with access in one org, to use the query() plugin, in a notebook cell, to run VQL queries on other orgs which they may not have access to. The user's permissions in the other org are the same as the permissions they have in the org containing the notebook.	8.0	More Details
CVE-2026-30615	A prompt injection vulnerability in Windsurf 1.9544.26 allows remote attackers to execute arbitrary commands on a victim system. When Windsurf processes attacker-controlled HTML content, malicious instructions can cause unauthorized modification of the local MCP configuration and automatic registration of a malicious MCP STDIO server, resulting in execution of arbitrary commands without further user interaction. Successful exploitation may allow attackers to execute commands on behalf of the user, persist malicious MCP configuration changes, and access sensitive information exposed through the application.	8.0	More Details
CVE-2026-33435	Weblate is a web based localization tool. In versions prior to 5.17, the project backup didn't filter Git and Mercurial configuration files which could lead to remote code execution under certain circumstances. This issue has been fixed in version 5.17. If developers are unable to update immediately, they can limit the scope of the vulnerability by restricting access to the project backup, as it is only accessible to users who can create projects.	8.0	More Details
CVE-2026-40321	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.2.2, a user could upload a specially crafted SVG file that could include scripts that can target both authenticated and unauthenticated DNN users. The impact is increased if the scripts are run by a power user. Version 10.2.2 patches the issue.	8.0	More Details
CVE-2025-65104	Firebird is an open-source relational database management system. In versions FB3 of the client library placed incorrect data length values into XSQLDA fields when communicating with FB4 or higher servers, resulting in an information leak. This issue is fixed by upgrading to the FB4 client or higher.	7.9	More Details
CVE-2026-5397	It has been identified that a vulnerability (CWE-427) exists in the UPS (Uninterruptible Power Supply) management application, whereby improper permissions on the installation directory allow a malicious actor to place a DLL that is then executed with administrator privileges. If a malicious DLL is placed in the installation directory of this product, there is a possibility that the malicious DLL may be executed by exploiting the product’s behavior of loading missing DLLs from the same directory as the executable during service startup.	7.8	More Details
CVE-2026-31368	AiAssistant is affected by type privilege bypass, successful exploitation of this vulnerability may affect service availability.	7.8	More Details
CVE-2025-36568	Dell PowerProtect Data Domain BoostFS for client of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an insufficiently protected credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to credential exposure. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account.	7.8	More Details
CVE-2026-35243	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF) executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF). CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2026-40527	radare2 prior to commit bc5a890 contains a command injection vulnerability in the afsv/afsvj command path where crafted ELF binaries can embed malicious r2 command sequences as DWARF DW_TAG_formal_parameter names. Attackers can craft a binary with shell commands in DWARF parameter names that execute when radare2 analyzes the binary with aaa and subsequently runs afsvj, allowing arbitrary shell command execution through the unsanitized parameter interpolation in the pfq command string.	7.8	More Details
CVE-2026-6776	Incorrect boundary conditions in the WebRTC: Networking component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.8	More Details
CVE-2026-29642	A local attacker who can execute privileged CSR operations (or can induce firmware to do so) performs carefully crafted reads/writes to menvcfg (e.g., csrrs in M-mode). On affected XiangShan versions (commit aecf601e803bfd2371667a3fb60bfcd83c333027, 2024-11-19), these menvcfg accesses can unexpectedly set WPRI (reserved) bits in the status view (xstatus) to 1. RISC-V defines WPRI fields as "writes preserve values, reads ignore values," i.e., they must not be modified by software manipulating other fields, and menvcfg itself contains multiple WPRI fields.	7.8	More Details
CVE-2026-30266	Insecure Permissions vulnerability in DeepCool DeepCreative v.1.2.7 and before allows a local attacker to execute arbitrary code via a crafted file	7.8	More Details
CVE-2026-4145	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix that could allow a local authenticated user to perform arbitrary code execution with elevated privileges.	7.8	More Details
CVE-2026-	Barracuda RMM versions prior to 2025.2.2 contain a privilege escalation vulnerability that allows local attackers to gain SYSTEM-level privileges by exploiting overly permissive filesystem ACLs on the C:\Windows\Automation directory. Attackers	7.8	More

22676	can modify existing automation content or place attacker-controlled files in this directory, which are then executed under the NT AUTHORITY\SYSTEM account during routine automation cycles, typically succeeding within the next execution cycle.		Details
CVE-2026-40176	Composer is a dependency manager for PHP. Versions 1.0 through 2.2.26 and 2.3 through 2.9.5 contain a command injection vulnerability in the Perforce::generateP4Command() method, which constructs shell commands by interpolating user-supplied Perforce connection parameters (port, user, client) without proper escaping. An attacker can inject arbitrary commands through these values in a malicious composer.json declaring a Perforce VCS repository, leading to command execution in the context of the user running Composer, even if Perforce is not installed. VCS repositories are only loaded from the root composer.json or the composer config directory, so this cannot be exploited through composer.json files of packages installed as dependencies. Users are at risk if they run Composer commands on untrusted projects with attacker-supplied composer.json files. This issue has been fixed in Composer 2.2.27 (2.2 LTS) and 2.9.6 (mainline).	7.8	More Details
CVE-2026-41295	OpenClaw before 2026.4.2 contains an improper trust boundary vulnerability allowing untrusted workspace channel shadows to execute during built-in channel setup and login. Attackers can clone a workspace with a malicious plugin claiming a bundled channel id to achieve unintended in-process code execution before the plugin is explicitly trusted.	7.8	More Details
CVE-2026-22619	Eaton Intelligent Power Protector (IPP) is affected by insecure library loading in its executable, which could lead to arbitrary code execution by an attacker with access to the software package. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download center.	7.8	More Details
CVE-2026-34428	Vvveb prior to 1.0.8.1 contains a server-side request forgery vulnerability in the oEmbedProxy action of the editor/editor module where the url parameter is passed directly to getUrl() via curl without scheme or destination validation. Authenticated backend users can supply file:// URLs to read arbitrary files readable by the web server process or http:// URLs targeting internal network addresses to probe internal services, with response bodies returned directly to the caller.	7.7	More Details
CVE-2026-41060	WWBN AVideo is an open source video platform. In versions 29.0 and below, the `isSSRFSafeURL()` function in `objects/functions.php` contains a same-domain shortcircuit (lines 4290-4296) that allows any URL whose hostname matches `webSiteRootURL` to bypass all SSRF protections. Because the check compares only the hostname and ignores the port, an attacker can reach arbitrary ports on the AVideo server by using the site's public hostname with a non-standard port. The response body is saved to a web-accessible path, enabling full exfiltration. Commit a0156a6398362086390d949190f9d52a823000ba fixes the issue.	7.7	More Details
CVE-2026-24177	NVIDIA KAI Scheduler contains a vulnerability where an attacker could access API endpoints without authorization. A successful exploit of this vulnerability might lead to information disclosure.	7.7	More Details
CVE-2026-32324	Anviz CX7 Firmware is vulnerable because the application embeds reusable certificate/key material, enabling decryption of MQTT traffic and potential interaction with device messaging channels at scale.	7.7	More Details
CVE-2026-40348	Movary is a self hosted web app to track and rate a user's watched movies. Prior to version 0.71.1, an ordinary authenticated user can trigger server-side requests to arbitrary internal targets through `POST /settings/jellyfin/server-url-verify`. The endpoint accepts a user-controlled URL, appends `/system/info/public`, and sends a server-side HTTP request with Guzzle. Because there is no restriction on internal hosts, loopback addresses, or private network ranges, this can be abused for SSRF and internal network probing. Any ordinary authenticated user can use this endpoint to make the server connect to arbitrary internal targets and distinguish between different network states. This enables SSRF-based internal reconnaissance, including host discovery, port-state probing, and service fingerprinting. In certain deployments, it may also be usable to reach internal administrative services or cloud metadata endpoints that are not directly accessible from the outside. Version 0.71.1 fixes the issue.	7.7	More Details
CVE-2026-40161	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. From 1.0.0 to 1.10.0, the Tekton Pipelines git resolver in API mode sends the system-configured Git API token to a user-controlled serverURL when the user omits the token parameter. A tenant with TaskRun or PipelineRun create permission can exfiltrate the shared API token (GitHub PAT, GitLab token, etc.) by pointing serverURL to an attacker-controlled endpoint.	7.7	More Details
CVE-2026-34242	Weblate is a web based localization tool. In versions prior to 5.17, the ZIP download feature didn't verify downloaded files, potentially following symlinks outside the repository. This issue has been fixed in version 5.17.	7.7	More Details
CVE-2026-40745	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in bdthemes Element Pack Elementor Addons bdthemes-element-pack-lite allows Blind SQL Injection.This issue affects Element Pack Elementor Addons: from n/a through <= 8.4.2.	7.6	More Details
CVE-2026-22011	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: ADPatch). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications DBA, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Applications DBA. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).	7.6	More Details
CVE-2026-41297	OpenClaw before 2026.3.31 contains a server-side request forgery vulnerability in the marketplace plugin download functionality that allows attackers to access internal resources by following unvalidated redirects. The marketplace.ts module fails to restrict redirect destinations during archive downloads, enabling remote attackers to redirect requests to arbitrary internal or external servers.	7.6	More Details
CVE-2025-63029	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WC Lovers WCFM Marketplace allows SQL Injection.This issue affects WCFM Marketplace: from n/a through 3.7.1.	7.6	More Details
CVE-	wger is a free, open-source workout and fitness manager. In versions 2.5 and below, the GymConfigUpdateView declares permission_required = 'config.change_gymconfig' but inherits WgerFormMixin instead of WgerPermissionMixin, so the		More

2026-40474	permission is never enforced at runtime. Since GymConfig is an ownerless singleton, any authenticated user can modify the global gym configuration, triggering save() side effects that bulk-update user profile gym assignments — a vertical privilege escalation to installation-wide configuration control. This issue is fixed in version 2.5.	7.6	Details
CVE-2026-23775	Dell PowerProtect Data Domain appliances with Data Domain Operating System (DD OS) of Feature Release versions 8.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to credential exposures. Authentication attempts as the compromised user would need to be authorized by a high privileged DD user. This vulnerability only affects systems with retention lock enabled.	7.6	More Details
CVE-2026-40589	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.214, a low-privileged agent can edit a visible customer and add an email address already owned by a hidden customer in another mailbox. The server discloses the hidden customer's name and profile URL in the success flash, reassigns the hidden email to the visible customer, and rebinds hidden-mailbox conversations for that email to the visible customer. Version 1.8.214 fixes the issue.	7.6	More Details
CVE-2026-41302	OpenClaw before 2026.3.31 contains a server-side request forgery vulnerability in the marketplace plugin download functionality that allows remote attackers to make arbitrary network requests. Attackers can exploit unguarded fetch() calls to access internal resources or interact with external services on behalf of the affected system.	7.6	More Details
CVE-2026-34320	Vulnerability in the Oracle Financial Services Customer Screening product of Oracle Financial Services Applications (component: User Interface). The supported version that is affected is 8.1.2.8.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Customer Screening. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Customer Screening accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-40870	Decidim is a participatory democracy framework. Starting in version 0.0.1 and prior to versions 0.30.5 and 0.31.1, the root level `commentable` field in the API allows access to all commentable resources within the platform, without any permission checks. All Decidim instances are impacted that have not secured the `/api` endpoint. The `/api` endpoint is publicly available with the default configuration. Versions 0.30.5 and 0.31.1 fix the issue. As a workaround, limit the scope to only authenticated users by limiting access to the `/api` endpoint. This would require custom code or installing the 3rd party module `Decidim::Apiauth`. With custom code, the `/api` endpoint can be limited to only authenticated users. The same configuration can be also used without the `allow` statements to disable all traffic to the the `/api` endpoint. When considering a workaround and the seriousness of the vulnerability, please consider the nature of the platform. If the platform is primarily serving public data, this vulnerability is not serious by its nature. If the platform is protecting some resources, e.g. inside private participation spaces, the vulnerability may expose some data to the attacker that is not meant public. For those who have enabled the organization setting "Force users to authenticate before access organization", the scope of this vulnerability is limited to the users who are allowed to log in to the Decidim platform. This setting was introduced in version 0.19.0 and it was applied to the `/api` endpoint in version 0.22.0.	7.5	More Details
CVE-2026-5426	Hard-coded ASP.NET/IIS machineKey value in Digital Knowledge KnowledgeDeliver deployments prior to February 24, 2026 allows adversaries to circumvent ViewState validation mechanisms and achieve remote code execution via malicious ViewState deserialization attacks	7.5	More Details
CVE-2026-34305	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-40869	Decidim is a participatory democracy framework. Starting in version 0.19.0 and prior to versions 0.30.5 and 0.31.1, a vulnerability allows any registered and authenticated user to accept or reject any amendments. The impact is on any users who have created proposals where the amendments feature is enabled. This also elevates the user accepting the amendment as the author of the original proposal as people amending proposals are provided coauthorship on the coauthorable resources. Versions 0.30.5 and 0.31.1 fix the issue. As a workaround, disable amendment reactions for the amendable component (e.g. proposals).	7.5	More Details
CVE-2024-2374	The XML parsers within multiple WSO2 products accept user-supplied XML data without properly configuring to prevent the resolution of external entities. This omission allows malicious actors to craft XML payloads that exploit the parser's behavior, leading to the inclusion of external resources. By leveraging this vulnerability, an attacker can read confidential files from the file system and access limited HTTP resources reachable by the product. Additionally, the vulnerability can be exploited to perform denial of service attacks by exhausting server resources through recursive entity expansion or fetching large external resources.	7.5	More Details
CVE-2026-3599	The Riaxe Product Customizer plugin for WordPress is vulnerable to SQL Injection via the 'options' parameter keys within 'product_data' of the /wp-json/InkXEProductDesignerLite/add-item-to-cart REST API endpoint in all versions up to, and including, 2.1.2. This is due to insufficient escaping on the user-supplied parameter and insufficient 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-2026-40890	The package `github.com/gomarkdown/markdown` is a Go library for parsing Markdown text and rendering as HTML. Processing a malformed input containing a < character that is not followed by a > character anywhere in the remaining text with a SmartypantsRenderer will lead to Out of Bounds read or a panic. This vulnerability is fixed with commit 759bbc3e32073c3bc4e25969c132fc520eda2778.	7.5	More Details
CVE-2026-35229	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.30 and 21.3-21.21. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details

CVE-2026-5050	The Payment Gateway for Redsys & WooCommerce Lite plugin for WordPress is vulnerable to Improper Verification of Cryptographic Signature in versions up to, and including, 7.0.0 due to successful_request() handlers calculating a local signature but not validating Ds_Signature from the request before accepting payment status across the Redsys, Bizum, and Google Pay gateway flows. This makes it possible for unauthenticated attackers to forge payment callback data and mark pending orders as paid when they know a valid order key and order amount, potentially allowing checkout completion and product or service fulfillment without a successful payment.	7.5	More Details
CVE-2026-35230	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2026-34310	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-35231	Vulnerability in the Oracle Financial Services Transaction Filtering product of Oracle Financial Services Applications (component: User Interface). The supported version that is affected is 8.1.2.8.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Transaction Filtering. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Transaction Filtering accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-40586	blueprintUE is a tool to help Unreal Engine developers. Prior to 4.2.0, the login form handler performs no throttling of any kind. Failed authentication attempts are processed at full network speed with no IP-based rate limiting, no per-account attempt counter, no temporary lockout, no progressive delay (Tarpit), and no CAPTCHA challenge. An attacker can submit an unlimited number of credential guesses. The password policy (10+ characters, mixed case, digit, special character) reduces the effective keyspace but does not prevent dictionary attacks, credential stuffing from breached databases, or targeted attacks against known users with predictable passwords. This vulnerability is fixed in 4.2.0.	7.5	More Details
CVE-2026-40247	free5GC is an open-source implementation of the 5G core network. In versions 4.2.1 and below of the UDR service, the handler for reading Traffic Influence Subscriptions checks whether the influenceId path segment equals subs-to-notify, but does not return after sending the HTTP 404 response when validation fails. Execution continues and the subscription data is returned alongside the 404 response. An unauthenticated attacker with access to the 5G Service Based Interface can read arbitrary Traffic Influence Subscriptions, including SUPIs/IMSIs, DNNs, S-NSSAIs, and callback URIs, by supplying any value for the influenceId path segment. A patched version was not available at the time of publication.	7.5	More Details
CVE-2026-31987	JWT Tokens used by tasks were exposed in logs. This could allow UI users to act as Dag Authors. Users are advised to upgrade to Airflow version that contains fix. Users are recommended to upgrade to version 3.2.0, which fixes this issue.	7.5	More Details
CVE-2026-40879	Nest is a framework for building scalable Node.js server-side applications. Prior to 11.1.19, when an attacker sends many small, valid JSON messages in one TCP frame, handleData() recurses once per message; the buffer shrinks each call. maxBufferSize is never reached; call stack overflows instead. A ~47 KB payload is sufficient to trigger RangeError. This vulnerability is fixed in 11.1.19.	7.5	More Details
CVE-2026-32965	Initialization of a resource with an insecure default vulnerability exists in SD-330AC and AMC Manager provided by silex technology, Inc. When the affected device is connected to the network with the initial (factory-default) configuration, the device can be configured with the null string password.	7.5	More Details
CVE-2026-6351	MailGates/MailAudit developed by Openfind has a CRLF Injection vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read system files.	7.5	More Details
CVE-2026-40613	Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.10.0, the STUN/TURN attribute parsing functions in coturn perform unsafe pointer casts from uint8_t * to uint16_t * without alignment checks. When processing a crafted STUN message with odd-aligned attribute boundaries, this results in misaligned memory reads at ns_turn_msg.c. On ARM64 architectures (AArch64) with strict alignment enforcement, this causes a SIGBUS signal that immediately kills the turnserver process. An unauthenticated remote attacker can crash any ARM64 coturn deployment by sending a single crafted UDP packet. This vulnerability is fixed in 4.10.0.	7.5	More Details
CVE-2026-3489	The DirectoryPress – Business Directory And Classified Ad Listing plugin for WordPress is vulnerable to SQL Injection via the 'packages' parameter in versions up to, and including, 3.6.26 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-2026-40170	ngtcp2 is a C implementation of the IETF QUIC protocol. In versions prior to 1.22.1, ngtcp2_qlog_parameters_set_transport_params() serializes peer transport parameters into a fixed 1024-byte stack buffer without bounds checking. When qlog is enabled, a remote peer can send sufficiently large transport parameters during the QUIC handshake to cause writes beyond the buffer boundary, resulting in a stack buffer overflow. This affects deployments that enable the qlog callback and process untrusted peer transport parameters. This issue has been fixed in version 1.22.1. If developers are unable to immediately upgrade, they can disable the qlog on client.	7.5	More Details
CVE-	free5GC is an open-source implementation of the 5G core network. In versions 1.4.2 and below of the UDR service, the handler for deleting Traffic Influence Subscriptions checks whether the influenceId path segment equals subs-to-notify, but		

2026-40246	does not return after sending the HTTP 404 response when validation fails. Execution continues and the subscription is deleted regardless. An unauthenticated attacker with access to the 5G Service Based Interface can delete arbitrary Traffic Influence Subscriptions by supplying any value for the influenceId path segment, while the API misleadingly returns a 404 Not Found response. A patched version was not available at the time of publication.	7.5	More Details
CVE-2026-29645	NEMU (OpenXiangShan/NEMU) before v2025.12.r2 contains an improper instruction-validation flaw in its RISC-V Vector (RVV) decoder. The decoder does not correctly validate the funct3 field when decoding vsetvli/vsetivli/vsetvl, allowing certain invalid OP-V instruction encodings to be misinterpreted and executed as vset* configuration instructions rather than raising an illegal-instruction exception. This can be exploited by providing crafted RISC-V binaries to cause incorrect trap behavior, architectural state corruption/divergence, and potential denial of service in systems that rely on NEMU for correct execution or sandboxing.	7.5	More Details
CVE-2026-25058	Vexa is an open-source, self-hostable meeting bot API and meeting transcription API. Prior to 0.10.0-260419-1910, the Vexa transcription-collector service exposes an internal endpoint `GET /internal/transcripts/{meeting_id}` that returns transcript data for any meeting without any authentication or authorization checks. An unauthenticated attacker can enumerate all meeting IDs, access any user's meeting transcripts without credentials, and steal confidential business conversations, passwords, and/or PII. Version 0.10.0-260419-1910 patches the issue.	7.5	More Details
CVE-2026-40303	zrok is software for sharing web services, files, and network resources. Prior to version 2.0.1, endpoints.GetSessionCookie parses an attacker-supplied cookie chunk count and calls make([]string, count) with no upper bound before any token validation occurs. The function is reached on every request to an OAuth-protected proxy share, allowing an unauthenticated remote attacker to trigger gigabyte-scale heap allocations per request, leading to process-level OOM termination or repeated goroutine panics. Both publicProxy and dynamicProxy are affected. Version 2.0.1 patches the issue.	7.5	More Details
CVE-2026-40515	OpenHarness before commit bd4df81 contains a permission bypass vulnerability that allows attackers to read sensitive files by exploiting incomplete path normalization in the permission checker. Attackers can invoke the built-in grep and glob tools with sensitive root directories that are not properly evaluated against configured path rules, allowing disclosure of sensitive local file content, key material, configuration files, or directory contents despite configured path restrictions.	7.5	More Details
CVE-2026-6784	Memory safety bugs present in Firefox 149 and Thunderbird 149. 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 150 and Thunderbird 150.	7.5	More Details
CVE-2026-30778	The SkyWalking OAP /debugging/config/dump endpoint may leak sensitive configuration information of MySQL/PostgreSQL. This issue affects Apache SkyWalking: from 9.7.0 through 10.3.0. Users are recommended to upgrade to version 10.4.0, which fixes the issue.	7.5	More Details
CVE-2026-5710	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Path Traversal leading to Arbitrary File Read in versions up to and including 1.3.9.6. This is due to the plugin using client-supplied mfile[] POST values as the source of truth for email attachment selection without performing any server-side upload provenance check, path canonicalization, or directory containment boundary enforcement. In dnd_wpcf7_posted_data(), each user-submitted filename is directly appended to the plugin's upload URL without sanitization. In dnd_cf7_mail_components(), the URL is converted back to a filesystem path using str_replace() and only file_exists() is used as the acceptance check before attaching the file to the outgoing CF7 email. This makes it possible for unauthenticated attackers to read and exfiltrate arbitrary files readable by the web server process via path traversal sequences in the mfile[] parameter, with files being disclosed as email attachments. Note: This vulnerability is limited to the 'wp-content' folder due to the wpcf7_is_file_path_in_content_dir() function in the Contact Form 7 plugin.	7.5	More Details
CVE-2026-6782	Information disclosure in the IP Protection component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	7.5	More Details
CVE-2026-6781	Denial-of-service in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	7.5	More Details
CVE-2026-6780	Denial-of-service in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	7.5	More Details
CVE-2024-33618	Uncontrolled Resource Consumption in Bosch VMS Central Server in Bosch VMS 12.0.1 allows attackers to consume excessive amounts of disk space via network interface.	7.5	More Details
CVE-2026-28212	Firebird is an open-source relational database management system. In versions prior to 6.0.0, 5.0.4, 4.0.7 and 3.0.14, when processing an op_slice network packet, the server passes an unprepared structure containing a null pointer to the SDL_info() function, resulting in a null pointer dereference and server crash. An unauthenticated attacker can trigger this by sending a crafted packet to the server port. This issue has been fixed in versions 6.0.0, 5.0.4, 4.0.7 and 3.0.14.	7.5	More Details
CVE-2026-6773	Denial-of-service due to integer overflow in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	7.5	More Details
CVE-2026-34282	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running	7.5	More Details

	sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).		
CVE-2026-6746	Use-after-free in the DOM: Core & HTML component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-6747	Use-after-free in the WebRTC component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-6749	Information disclosure due to uninitialized memory in the Graphics: Canvas2D component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-33337	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, when deserializing a slice packet, the xdr_datum() function does not validate that a cstring length conforms to the slice descriptor bounds, allowing a cstring longer than the allocated buffer to overflow it. An unauthenticated attacker can exploit this by sending a crafted packet to the server, potentially causing a crash or other security impact. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	7.5	More Details
CVE-2026-40461	Anviz CX2 Lite and CX7 are vulnerable to unauthenticated POST requests that modify debug settings (e.g., enabling SSH), allowing unauthorized state changes that can facilitate later compromise.	7.5	More Details
CVE-2026-5088	Apache::API::Password versions through v0.5.2 for Perl can generate insecure random values for salts. The _make_salt and _make_salt_bcrypt methods will attept to load Crypt::URandom and then Bytes::Random::Secure to generate random bytes for the salt. If those modules are unavailable, it will simply return 16 bytes generated with Perl's built-in rand function. The rand function is unsuitable for cryptographic use. These salts are used for password hashing.	7.5	More Details
CVE-2026-40719	Deadwood in MaraDNS 3.5.0036 allows attackers to exhaust connection slots via a zone whose authoritative nameserver address cannot be resolved.	7.5	More Details
CVE-2026-6772	Incorrect boundary conditions in the Libraries component in NSS. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-6754	Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-6758	Use-after-free in the JavaScript: WebAssembly component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	7.5	More Details
CVE-2026-35215	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, the sdl_desc() function does not validate the length of a decoded SDL descriptor from a slice packet. A zero-length descriptor is later used to calculate the number of slice items, causing a division by zero. An unauthenticated attacker can exploit this by sending a crafted slice packet to crash the server. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	7.5	More Details
CVE-2026-33806	Impact: Fastify applications using schema.body.content for per-content-type body validation can have validation bypassed entirely by prepending a space to the Content-Type header. The body is still parsed correctly but schema validation is skipped. This is a regression introduced in fastify >= 5.3.2 by the fix for CVE-2025-32442 Patches: Upgrade to fastify v5.8.5 or later. Workarounds: None. Upgrade to the patched version.	7.5	More Details
CVE-2026-32650	Anviz CrossChex Standard is vulnerable when an attacker manipulates the TDS7 PreLogin to disable encryption, causing database credentials to be sent in plaintext and enabling unauthorized database access.	7.5	More Details
CVE-2026-6759	Use-after-free in the Widget: Cocoa component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-6766	Incorrect boundary conditions in the Libraries component in NSS. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.5	More Details
CVE-2026-34232	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, the xdr_status_vector() function does not handle the isc_arg_cstring type when decoding an op_response packet, causing a server crash when one is encountered in the status vector. An unauthenticated attacker can exploit this by sending a crafted op_response packet to the server. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	7.5	More Details
CVE-2026-40286	WeGIA is a web manager for charitable institutions. In versions prior to 3.6.10, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the 'Member Registration' (Cadastrar Sócio) function. By injecting a payload into the 'Member Name' (Nome Sócio) field, the script is persistently stored in the database. Consequently, the payload is executed whenever a user navigates to certain URL. Version 3.6.10 fixes the issue.	7.5	More Details
CVE-2026-31317	Craftql v1.3.7 and before is vulnerable to Server-Side Request Forgery (SSRF) which allows an attacker to execute arbitrary code via the vendor/markhuot/craftql/src/Listeners/GetAssetsFieldSchema.php file	7.5	More Details

CVE-2026-40245	Free5GC is an open-source Linux Foundation project for 5th generation (5G) mobile core networks. Versions 4.2.1 and below contain an information disclosure vulnerability in the UDR (Unified Data Repository) service. The handler for GET /nudr-dr/v2/application-data/influenceData/subs-to-notify sends an HTTP 400 error response when required query parameters are missing but does not return afterward. Execution continues into the processor function, which queries the data repository and appends the full list of Traffic Influence Subscriptions, including SUPI/IMSI values, to the response body. An unauthenticated attacker with network access to the 5G Service Based Interface can retrieve stored subscriber identifiers with a single parameterless HTTP GET request. The SUPI is the most sensitive subscriber identifier in 5G networks, and its exposure undermines the privacy guarantees of the 3GPP SUCI concealment mechanism at the core network level. A similar bypass exists when sending a malformed snssai parameter due to the same missing return pattern.	7.5	More Details
CVE-2026-39320	Signal K Server is a server application that runs on a central hub in a boat. Versions prior to 2.25.0 are vulnerable to an unauthenticated Regular Expression Denial of Service (ReDoS) attack within the WebSocket subscription handling logic. By injecting unescaped regex metacharacters into the `context` parameter of a stream subscription, an attacker can force the server's Node.js event loop into a catastrophic backtracking loop when evaluating long string identifiers (like the server's self UUID). This results in a total Denial of Service (DoS) where the server CPU spikes to 100% and becomes completely unresponsive to further API or socket requests. Version 2.25.0 contains a fix.	7.5	More Details
CVE-2026-4525	If a Vault auth mount is configured to pass through the "Authorization" header, and the "Authorization" header is used to authenticate to Vault, Vault forwarded the Vault token to the auth plugin backend. Fixed in 2.0.0, 1.21.5, 1.20.10, and 1.19.16.	7.5	More Details
CVE-2026-35242	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2026-32228	UI / API User with asset materialize permission could trigger dags they had no access to. Users are advised to migrate to Airflow version 3.2.0 that fixes the issue.	7.5	More Details
CVE-2026-30912	In case of SQL errors, exception/stack trace of errors was exposed in API even if "api/expose_stack_traces" was set to false. That could lead to exposing additional information to potential attacker. Users are recommended to upgrade to Apache Airflow 3.2.0, which fixes the issue.	7.5	More Details
CVE-2026-5807	Vault is vulnerable to a denial-of-service condition where an unauthenticated attacker can repeatedly initiate or cancel root token generation or rekey operations, occupying the single in-progress operation slot. This prevents legitimate operators from completing these workflows. This vulnerability, CVE-2026-5807, is fixed in Vault Community Edition 2.0.0 and Vault Enterprise 2.0.0.	7.5	More Details
CVE-2026-6319	Use after free in Payments in Google Chrome on Android prior to 147.0.7727.101 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: Medium)	7.5	More Details
CVE-2026-6308	Out of bounds read in Media in Google Chrome prior to 147.0.7727.101 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)	7.5	More Details
CVE-2026-35245	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-4659	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to Arbitrary File Read via the Repeater JSON/CSV URL parameter in versions up to, and including, 2.0.6. This is due to insufficient path traversal sanitization in the URLtoRelative() and urlToPath() functions, combined with the ability to enable debug output in widget settings. The URLtoRelative() function only performs a simple string replacement to remove the site's base URL without sanitizing path traversal sequences (../), and the cleanPath() function only normalizes directory separators without removing traversal components. This allows an attacker to provide a URL like http://site.com/../../../../etc/passwd which, after URLtoRelative() strips the domain, results in /../../../../etc/passwd being concatenated with the base path and ultimately resolved to /etc/passwd. This makes it possible for authenticated attackers with Author-level access and above to read arbitrary local files from the WordPress host, including sensitive files such as wp-config.	7.5	More Details
CVE-2026-35465	SecureDrop Client is a desktop app for journalists to securely communicate with sources and handle submissions on the SecureDrop Workstation. In versions 0.17.4 and below, a compromised SecureDrop Server can achieve code execution on the Client's virtual machine (sd-app) by exploiting improper filename validation in gzip archive extraction, which permits absolute paths and enables overwriting critical files like the SQLite database. Exploitation requires prior compromise of the dedicated SecureDrop Server, which itself is hardened and only accessible via Tor hidden services. Despite the high attack complexity, the vulnerability is rated High severity due to its significant impact on confidentiality, integrity, and availability of decrypted source submissions. This issue is similar to CVE-2025-24888 but occurs through a different code path, and a more robust fix has been implemented in the replacement SecureDrop Inbox codebase. The issue has been fixed in version 0.17.5.	7.5	More Details
CVE-2026-35246	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details

CVE-2026-39111	SQL Injection vulnerability in Apartment Visitors Management System Apartment Visitors Management System V1.1 in the email parameter of the forgot password page (forgot-password.php). This allows an unauthenticated attacker to manipulate backend SQL queries and retrieve sensitive user data.	7.5	More Details
CVE-2026-35251	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2026-34297	Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Knowledge Integration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-2262	The Easy Appointments plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.12.21 via the `/wp-json/wp/v2/eablocks/ea_appointments/` REST API endpoint. This is due to the endpoint being registered with `'permission_callback' => '__return_true'`, which allows access without any authentication or authorization checks. This makes it possible for unauthenticated attackers to extract sensitive customer appointment data including full names, email addresses, phone numbers, IP addresses, appointment descriptions, and pricing information.	7.5	More Details
CVE-2026-6372	Missing Authorization vulnerability in Plisio Accept Cryptocurrencies with Plisio allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Accept Cryptocurrencies with Plisio: from n/a through 2.0.5.	7.5	More Details
CVE-2026-30996	An issue in the file handling logic of the component download.php of SAC-NFe v2.0.02 allows attackers to execute a directory traversal and read arbitrary files from the system via a crafted GET request.	7.5	More Details
CVE-2026-30994	Incorrect access control in the config.php component of Slah v1.5.0 and below allows unauthenticated attackers to access sensitive information, including active session credentials.	7.5	More Details
CVE-2026-33626	LMDeploy is a toolkit for compressing, deploying, and serving large language models. Versions prior to 0.12.3 have a Server-Side Request Forgery (SSRF) vulnerability in LMDeploy's vision-language module. The `load_image()` function in `lmdeploy/vl/utils.py` fetches arbitrary URLs without validating internal/private IP addresses, allowing attackers to access cloud metadata services, internal networks, and sensitive resources. Version 0.12.3 patches the issue.	7.5	More Details
CVE-2026-5928	Calling the ungetwc function on a FILE stream with wide characters encoded in a character set that has overlaps between its single byte and multi-byte character encodings, in the GNU C Library version 2.43 or earlier, may result in an attempt to read bytes before an allocated buffer, potentially resulting in unintentional disclosure of neighboring data in the heap, or a program crash. A bug in the wide character pushback implementation (_IO_wdefault_pbackfail in libio/wgenops.c) causes ungetwc() to operate on the regular character buffer (fp->_IO_read_ptr) instead of the actual wide-stream read pointer (fp->_wide_data->_IO_read_ptr). The program crash may happen in cases where fp->_IO_read_ptr is not initialized and hence points to NULL. The buffer under-read requires a special situation where the input character encoding is such that there are overlaps between single byte representations and multibyte representations in that encoding, resulting in spurious matches. The spurious match case is not possible in the standard Unicode character sets.	7.5	More Details
CVE-2026-22010	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-22016	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-34290	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Identity Manager Connector. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2025-67841	Nordic Semiconductor IronSide SE for nRF54H20 before 23.0.2+17 has an Algorithmic complexity issue.	7.5	More Details

CVE-2026-40938	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. From 1.0.0 to before 1.11.0, the git resolver's revision parameter is passed directly as a positional argument to git fetch without any validation that it does not begin with a - character. Because git parses flags from mixed positional arguments, an attacker can inject arbitrary git fetch flags such as --upload-pack=<binary>. Combined with the validateRepoURL function explicitly permitting URLs that begin with / (local filesystem paths), a tenant who can submit ResolutionRequest objects can chain these two behaviors to execute an arbitrary binary on the resolver pod. The tekton-pipelines-resolvers ServiceAccount holds cluster-wide get/list/watch on all Secrets, so code execution on the resolver pod enables full cluster-wide secret exfiltration. This vulnerability is fixed in 1.11.1.	7.5	More Details
CVE-2026-30364	CentSDR commit e40795 was discovered to contain a stack overflow in the "Thread1" function.	7.5	More Details
CVE-2026-6507	A flaw was found in dnsmasq. A remote attacker could exploit an out-of-bounds write vulnerability by sending a specially crafted BOOTREPLY (Bootstrap Protocol Reply) packet to a dnsmasq server configured with the `--dhcp-split-relay` option. This can lead to memory corruption, causing the dnsmasq daemon to crash and resulting in a denial of service (DoS).	7.5	More Details
CVE-2026-30656	A NULL pointer dereference vulnerability exists in fio (Flexible I/O Tester) v3.41 when parsing job files containing the fdp_pli option. The callback function str_fdp_pli_cb() does not validate the input pointer and calls strdup() on a NULL value when the option is specified without an argument. This results in a segmentation fault and process crash.	7.5	More Details
CVE-2026-41015	radare2 before 9236f44, when configured on UNIX without SSL, allows command injection via a PDB name to rabin2 -PP. NOTE: although users are supposed to use the latest version from git (not a release), the date range for the vulnerable code was less than a week, occurring after 6.1.2 but before 6.1.3.	7.4	More Details
CVE-2026-40585	blueprintUE is a tool to help Unreal Engine developers. Prior to 4.2.0, when a password reset is initiated, a 128-character CSPRNG token is generated and stored alongside a password_reset_at timestamp. However, the token redemption function findUserIDFromEmailAndToken() queries only for a matching email + password_reset token pair — it does not check whether the password_reset_at timestamp has elapsed any maximum window. A generated reset token is valid indefinitely until it is explicitly consumed or overwritten by a subsequent reset request. This vulnerability is fixed in 4.2.0.	7.4	More Details
CVE-2026-33804	@fastify/middie versions 9.3.1 and earlier are vulnerable to middleware bypass when the deprecated Fastify ignoreDuplicateSlashes option is enabled. The middleware path matching logic does not account for duplicate slash normalization performed by Fastify's router, allowing requests with duplicate slashes to bypass middleware authentication and authorization checks. This only affects applications using the deprecated ignoreDuplicateSlashes option. Upgrade to @fastify/middie 9.3.2 to fix this issue. There are no workarounds other than disabling the ignoreDuplicateSlashes option.	7.4	More Details
CVE-2026-33667	OpenProject is an open-source project management application. In versions prior to 17.3.0, 2FA OTP verification in the confirm_otp action of the two_factor_authentication module has no rate limiting, lockout mechanism, or failed-attempt tracking. The existing brute_force_block_after_failed_logins setting only counts password login failures and does not apply to the 2FA verification stage, and neither the fail_login nor stage_failure methods increment any counter, lock the account, or add any delay. With the default TOTP drift window of ±60 seconds allowing approximately 5 valid codes at any time, an attacker who knows a user's password can brute-force the 6-digit TOTP code at roughly 5-10 attempts per second with an expected completion time of approximately 11 hours. The same vulnerability applies to backup code verification. This effectively allows complete 2FA bypass for any account where the password is known. This issue has been fixed in version 17.3.0.	7.4	More Details
CVE-2026-32631	Git for Windows is the Windows port of Git. Versions prior to 2.53.0.windows.3 do not have protections that prevent attackers from obtaining a user's NTLM hash. The NTLM hash can be obtained by tricking users into cloning a malicious repository, or checking out a malicious branch, that accesses an attacker-controlled server. By default, NTLM authentication does not need any user interaction. By brute-forcing the NTLMv2 hash (which is expensive, but possible), credentials can be extracted. This issue has been fixed in version 2.53.0.windows.3.	7.4	More Details
CVE-2026-41035	In rsync 3.0.1 through 3.4.1, receive_xattr relies on an untrusted length value during a qsort call, leading to a receiver use-after-free. The victim must run rsync with -X (aka --xattrs). On Linux, many (but not all) common configurations are vulnerable. Non-Linux platforms are more widely vulnerable.	7.4	More Details
CVE-2026-0972	The login limit is not enforced on the SFTP service of Fortra's GoAnywhere MFT prior to 7.10.0 if the Web User attempting to be logged in to is configured to log in with an SSH Key, making the SSH key vulnerable to being guessed via Brute Force.	7.3	More Details
CVE-2026-6568	A vulnerability was determined in kodcloud KodExplorer up to 4.52. This affects the function share.class.php::initShareOld of the file /app/controller/share.class.php of the component Public Share Handler. This manipulation of the argument path causes path traversal. 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-2026-6621	A vulnerability was determined in 1024bit extend-deep up to 0.1.6. The impacted element is an unknown function of the file index.js. This manipulation of the argument __proto__ causes improperly controlled modification of object prototype attributes. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The code repository of the project has not been active for many years.	7.3	More Details
CVE-2026-6580	A security vulnerability has been detected in liangliangyy DjangoBlog up to 2.1.0.0. Affected is an unknown function of the file owntracks/views.py of the component Amap API Call Handler. Such manipulation of the argument key leads to use of hard-coded cryptographic key . The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6752	Incorrect boundary conditions in the WebRTC component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.3	More Details
CVE-2026-	A vulnerability was identified in liangliangyy DjangoBlog up to 2.1.0.0. The impacted element is an unknown function of the file owntracks/views.py of the component logtracks Endpoint. The manipulation leads to missing authentication. The attack	7.3	More

6577	can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2026-6751	Uninitialized memory in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	7.3	More Details
CVE-2026-6574	A vulnerability has been found in osuuu LightPicture up to 1.2.2. This issue affects some unknown processing of the file /public/install/lp.sql of the component API Upload Endpoint. Such manipulation of the argument key leads to hard-coded credentials. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6625	A security vulnerability has been detected in moxi624 Mogu Blog v2 up to 5.2. Affected by this vulnerability is the function LocalFileServiceImpl.uploadPictureByUrl of the file mogu_picture/src/main/java/com/moxi/mogublog/picture/service/impl/LocalFileServiceImpl.java of the component Picture Storage Service. The manipulation leads to server-side request forgery. 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.	7.3	More Details
CVE-2026-6629	A vulnerability has been found in Metasoft 美特软件 MetaCRM up to 6.4.0. This vulnerability affects the function Statement.executeUpdate of the file sql.jsp of the component Interface. Such manipulation of the argument sql leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6569	A vulnerability was identified in kodcloud KodExplorer up to 4.52. This impacts the function fileGet of the file /app/controller/share.class.php of the component fileGet Endpoint. Such manipulation of the argument fileUrl leads to improper authentication. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6635	A security vulnerability has been detected in rowboatlabs rowboat up to 0.1.67. This impacts the function tool_call of the file apps/experimental/tools_webhook/app.py of the component tools_webhook. Such manipulation of the argument X-Tools-JWE leads to improper authentication. 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.	7.3	More Details
CVE-2026-30616	Jaaz 1.0.30 contains a remote code execution vulnerability in its MCP STDIO command execution handling. A remote attacker can send crafted network requests to the network-accessible Jaaz application, causing attacker-controlled commands to be executed on the server. Successful exploitation results in arbitrary command execution within the context of the Jaaz service, potentially allowing full compromise of the affected system.	7.3	More Details
CVE-2026-6562	A flaw has been found in dameng100 muucmf 1.9.5.20260309. Impacted is the function getListByPage of the file /index/Search/index.html. Executing a manipulation of the argument keyword can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6615	A weakness has been identified in TransformerOptimus SuperAGI up to 0.0.14. Affected by this issue is the function Upload of the file superagi/controllers/resources.py of the component Multipart Upload Handler. This manipulation of the argument Name causes path traversal. It is possible to initiate the attack 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.	7.3	More Details
CVE-2026-37337	SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_playlist.php.	7.3	More Details
CVE-2025-14362	The login limit is not enforced on the SFTP service of Fortra's GoAnywhere MFT prior to 7.10.0 if the Web User attempting to be logged in to is configured to log in with an SSH Key, making the SSH key vulnerable to being guessed via Brute Force.	7.3	More Details
CVE-2026-6662	A vulnerability was found in ericc-ch copilot-api up to 0.7.0. The impacted element is the function cors of the file src/server.ts of the component Token Endpoint. Performing a manipulation results in permissive cross-domain policy with untrusted domains. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-38834	Tenda W30E V2.0 V16.01.0.21 was found to contain a command injection vulnerability in the do_ping_action function via the hostName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	7.3	More Details
CVE-2026-4134	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix, that during installation could allow a local authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2026-21733	Software installed and run as a non-privileged user may conduct improper GPU system calls to gain write permission to read-only wrapped user-mode memory and files. This is caused by improper handling of GPU memory reservation protections.	7.3	More Details
CVE-2026-6490	A weakness has been identified in QueryMine sms up to 7ab5a9ea196209611134525ffc18de25c57d9593. Impacted is an unknown function of the file admin/deletecourse.php of the component GET Request Parameter Handler. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-	A flaw was found in gimp. This buffer overflow vulnerability in the GIF image loading component's `ReadJeffsImage` function allows an attacker to write beyond an allocated buffer by processing a specially crafted GIF file. This can lead to a denial of	7.3	More

6384	service or potentially arbitrary code execution.		Details
CVE-2026-37336	SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_music.php.	7.3	More Details
CVE-2026-6582	A flaw has been found in TransformerOptimus SuperAGI up to 0.0.14. Affected by this issue is the function get_vector_db_details of the file superagi/controllers/vector_dbs.py of the component Vector Database Management Endpoint. Executing a manipulation can lead to missing authentication. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6594	A vulnerability was determined in brikcss merge up to 1.3.0. This affects an unknown part. Executing a manipulation of the argument __proto__/constructor.prototype/prototype can lead to improperly controlled modification of object prototype attributes. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6596	A security flaw has been discovered in langflow-ai langflow up to 1.1.0. This issue affects the function create_upload_file of the file src/backend/base/Langflow/api/v1/endpoints.py of the component API Endpoint. The manipulation results in unrestricted upload. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6595	A vulnerability was identified in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This vulnerability affects unknown code of the file buslocation.php of the component HTTP GET Parameter Handler. The manipulation of the argument bus_id leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6603	A vulnerability was determined in modelscope agentscope up to 1.0.18. Affected by this vulnerability is the function execute_python_code/execute_shell_command of the file src/AgentScope/tool/_coding/_python.py. This manipulation causes code injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-41082	In OCaml opam before 2.5.1, a .install field containing a destination filepath can use ../ to reach a parent directory.	7.3	More Details
CVE-2026-6602	A vulnerability was found in rickxy Hospital Management System up to 88a4290d957dc5bdde8a56e5ad451ad14f7f90f4. Affected is an unknown function of the file /backend/admin/his_admin_account.php. The manipulation of the argument ad_dpic results in unrestricted upload. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable.	7.3	More Details
CVE-2026-6604	A vulnerability was identified in modelscope agentscope up to 1.0.18. Affected by this issue is the function _parse_url/prepare_image/openai_audio_to_text of the file src/agentscope/tool/_multi_modality/_openai_tools.py of the component Cloud Metadata Endpoint. Such manipulation of the argument image_url/audio_file_url leads to server-side request forgery. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6605	A security flaw has been discovered in modelscope agentscope up to 1.0.18. This affects the function _get_bytes_from_web_url of the file src/agentscope/_utils/_common.py of the component Internal Service. Performing a manipulation results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-6606	A weakness has been identified in modelscope agentscope up to 1.0.18. This vulnerability affects the function _process_audio_block of the file src/agentscope/agent/_agent_base.py. Executing a manipulation of the argument url can lead to server-side request forgery. It is possible to launch the attack 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.	7.3	More Details
CVE-2026-23772	Dell Storage Manager - Replay Manager for Microsoft Servers, version(s) 8.0, contain(s) an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.3	More Details
CVE-2026-24506	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution as root.	7.2	More Details
CVE-2026-2834	The Age Verification & Identity Verification by Token of Trust plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'description' parameter in all versions up to, and including, 3.32.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-24505	Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	7.2	More Details
CVE-2026-40520	FreePBX api module version 17.0.8 and prior contain a command injection vulnerability in the initiateGqlAPIProcess() function where GraphQL mutation input fields are passed directly to shell_exec() without sanitization or escaping. An authenticated user with a valid bearer token can send a GraphQL moduleOperations mutation with backtick-wrapped commands in the	7.2	More Details

	module field to execute arbitrary commands on the underlying host as the web server user.		
CVE-2026-40871	mailcow: dockerized is an open source groupware/email suite based on docker. Versions prior to 2026-03b have a second-order SQL injection vulnerability in the quarantine_category field via the Mailcow API. The /api/v1/add/mailbox endpoint stores quarantine_category without validation or sanitization. This value is later used by quarantine_notify.py, which constructs SQL queries using unsafe % string formatting instead of parameterized queries. This results in a delayed (second-order) SQL injection when the quarantine notification job executes, allowing an attacker to inject arbitrary SQL. Using a UNION SELECT, sensitive data (e.g., admin credentials) can be exfiltrated and rendered inside quarantine notification emails. Version 2026-03b fixes the vulnerability.	7.2	More Details
CVE-2026-24504	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	7.2	More Details
CVE-2026-33392	In JetBrains YouTrack before 2025.3.131383 high privileged user can achieve RCE via sandbox bypass	7.2	More Details
CVE-2026-6361	Heap buffer overflow in PDFium in Google Chrome on Windows prior to 147.0.7727.101 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	7.2	More Details
CVE-2026-5231	The WP Statistics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'utm_source' parameter in all versions up to, and including, 14.16.4. This is due to insufficient input sanitization and output escaping. The plugin's referral parser copies the raw utm_source value into the source_name field when a wildcard channel domain matches, and the chart renderer later inserts this value into legend markup via innerHTML without escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in admin pages that will execute whenever an administrator accesses the Referrals Overview or Social Media analytics pages.	7.2	More Details
CVE-2026-39467	Deserialization of Untrusted Data vulnerability in MetaSlider Responsive Slider by MetaSlider allows Object Injection.This issue affects Responsive Slider by MetaSlider: from n/a through 3.106.0.	7.2	More Details
CVE-2026-5694	The Quick Interest Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'loan-amount' and 'loan-period' parameters in all versions up to, and including, 3.1.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-3876	The Prismatic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'prismatic_encoded' pseudo-shortcode in all versions up to, and including, 3.7.3. This is due to insufficient input sanitization and output escaping on user-supplied attributes within the 'prismatic_decode' function. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page by submitting a comment containing a crafted 'prismatic_encoded' pseudo-shortcode.	7.2	More Details
CVE-2026-37344	SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/manage_location.php.	7.2	More Details
CVE-2026-37343	SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/manage_user.php.	7.2	More Details
CVE-2026-23774	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	7.2	More Details
CVE-2026-20205	In Splunk MCP Server app versions below 1.0.3 , a user who holds a role with access to the Splunk `_internal` index or possesses the high-privilege capability `mcp_tool_admin` could view users session and authorization tokens in clear text. The vulnerability would require either local access to the log files or administrative access to internal indexes, which by default only the admin role receives. Review roles and capabilities on your instance and restrict internal index access to administrator-level roles. See [Define roles on the Splunk platform with capabilities] (https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities) and [Connecting to MCP Server and Admin settings](https://help.splunk.com/en/splunk-enterprise/mcp-server-for-splunk-platform/connecting-to-mcp-server-and-admin-settings) in the Splunk documentation for more information.	7.2	More Details
CVE-2026-6483	A vulnerability was found in Wavlink WL-WN530H4 20220721. This vulnerability affects the function strcat/snprintf of the file /cgi-bin/internet.cgi. The manipulation results in os command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. Upgrading to version 2026.04.16 is able to resolve this issue. Upgrading the affected component is recommended.	7.2	More Details
CVE-2026-34292	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-37341	SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/manage_category.php.	7.2	More Details

CVE-2026-37342	SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/view_parked_details.php.	7.2	More Details
CVE-2026-23776	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain(s) an Improper Certificate Validation vulnerability in certificate-based login. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.2	More Details
CVE-2026-39971	Serendipity is a PHP-powered weblog engine. In versions 2.6-beta2 and below, the email sending functionality in include/functions.inc.php inserts $_SERVER['HTTP_HOST'] directly into the Message-ID SMTP header without validation, and the existing sanitization function serendipity_isResponseClean() is not called on HTTP_HOST before embedding it. An attacker who can control the Host header during an email-triggering action such as comment notifications or subscription emails can inject arbitrary SMTP headers into outgoing emails. This enables identity spoofing, reply hijacking via manipulated Message-ID threading, and email reputation abuse through the attacker's domain being embedded in legitimate mail headers. This issue has been fixed in version 2.6.0.	7.2	More Details
CVE-2026-23778	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability to gain root-level access.	7.2	More Details
CVE-2026-37748	Visitor Management System 1.0 by sanjay1313 is vulnerable to Unrestricted File Upload in vms/php/admin_user_insert.php and vms/php/update_1.php. The move_uploaded_file() function is called without any MIME type, extension, or content validation, allowing an authenticated admin to upload a PHP webshell and achieve Remote Code Execution on the server.	7.2	More Details
CVE-2026-3643	The Accessibly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the REST API in all versions up to, and including, 3.0.3. The plugin registers REST API endpoints at `/otm-ac/v1/update-widget-options` and `/otm-ac/v1/update-app-config` with the `permission_callback` set to `__return_true`, which means no authentication or authorization check is performed. The `updateWidgetOptions()` function in `AdminApi.php` accepts user-supplied JSON data and passes it directly to `AccessiblyOptions::updateAppConfig()`, which saves it to the WordPress options table via `update_option()` without any sanitization or validation. The stored `widgetSrc` value is later retrieved by `AssetsManager::enqueueFrontendScripts()` and passed directly to `wp_enqueue_script()` as the script URL, causing it to be rendered as a `<script>` tag on every front-end page. This makes it possible for unauthenticated attackers to inject arbitrary JavaScript that executes for all site visitors by changing the `widgetSrc` option to point to a malicious external script.	7.2	More Details
CVE-2026-26943	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	7.2	More Details
CVE-2026-29643	XiangShan (Open-source high-performance RISC-V processor) commit edb1dfaf7d290ae99724594507dc46c2c2125384 (2024-11-28) contains an improper exceptional-condition handling flaw in its CSR subsystem (NewCSR). On affected versions, certain sequences of CSR operations targeting non-existent/custom CSR addresses may trigger an illegal-instruction exception but fail to reliably transfer control to the configured trap handler (mtvec), causing control-flow disruption and potentially leaving the core in a hung or unrecoverable state. This can be exploited by a local attacker able to execute code on the processor to cause a denial of service and potentially inconsistent architectural state.	7.1	More Details
CVE-2026-39973	Apktool is a tool for reverse engineering Android APK files. In versions 3.0.0 and 3.0.1, a path traversal vulnerability in `brut/androlib/res/decoder/ResFileDecoder.java` allows a maliciously crafted APK to write arbitrary files to the filesystem during standard decoding (`apktool d`). This is a security regression introduced in commit e10a045 (PR #4041, December 12, 2025), which removed the `BrutIO.sanitizePath()` call that previously prevented path traversal in resource file output paths. An attacker can embed `../` sequences in the `resources.arsc` Type String Pool to escape the output directory and write files to arbitrary locations, including `~/.ssh/config`, `~/.bashrc`, or Windows Startup folders, escalating to RCE. The fix in version 3.0.2 re-introduces `BrutIO.sanitizePath()` in `ResFileDecoder.java` before file write operations.	7.1	More Details
CVE-2026-0827	During an internal security assessment, a potential vulnerability was discovered in Lenovo Diagnostics and the HardwareScanAddin used in Lenovo Vantage that, during installation or when using hardware scan, could allow a local authenticated user to perform an arbitrary file write with elevated privileges.	7.1	More Details
CVE-2026-30459	An issue in the Forgot Password feature of Daylight Studio FuelCMS v1.5.2 allows unauthenticated attackers to obtain the password reset token of a victim user via a crafted link placed in a valid e-mail message.	7.1	More Details
CVE-2026-20204	In Splunk Enterprise versions below 10.2.1, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.5, 10.2.2510.9, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles could potentially perform a Remote Code Execution (RCE) by uploading a malicious file to the `$SPLUNK_HOME/var/run/splunk/apptemp` directory due to improper handling and insufficient isolation of temporary files within the `apptemp` directory.	7.1	More Details
CVE-2026-41299	OpenClaw before 2026.3.28 contains an authorization bypass vulnerability in the chat.send gateway method where ACP-only provenance fields are gated by self-declared client metadata from WebSocket handshake rather than verified authorization state. Authenticated operator clients can spoof ACP identity labels and inject reserved provenance fields intended only for the ACP bridge by manipulating client metadata during connection.	7.1	More Details
CVE-2026-41192	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, the reply and draft flows trust client-supplied encrypted attachment IDs. Any IDs present in `attachments_all[]` but omitted from retained lists are decrypted and passed directly to `Attachment::deleteByIds()`. Because `load_attachments` returns encrypted IDs for attachments on a visible conversation, a mailbox peer can replay those IDs through `save_draft` and delete the original attachment row and file. Version 1.8.215 fixes the vulnerability.	7.1	More Details
	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, `MailboxesController::updateSave()`		

CVE-2026-41191	persists `chat_start_new` outside the allowed-field filter. A user with only the mailbox `sig` permission sees only the signature field in the UI, but can still change the hidden mailbox-wide chat setting via direct POST. Version 1.8.215 fixes the vulnerability.	7.1	More Details
CVE-2026-41190	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, when `APP_SHOW_ONLY_ASSIGNED_CONVERSATIONS` is enabled, direct conversation view correctly blocks users who are neither the assignee nor the creator. The `save_draft` AJAX path is weaker. A direct POST can create a draft inside a conversation that is hidden in the UI. Version 1.8.215 fixes the vulnerability.	7.1	More Details
CVE-2026-41057	WWBN AVideo is an open source video platform. In versions 29.0 and below, the CORS origin validation fix in commit `986e64aad` is incomplete. Two separate code paths still reflect arbitrary `Origin` headers with credentials allowed for all `/api/*` endpoints: (1) `plugin/API/router.php` lines 4-8 unconditionally reflect any origin before application code runs, and (2) `allowOrigin(true)` called by `get.json.php` and `set.json.php` reflects any origin with `Access-Control-Allow-Credentials: true`. An attacker can make cross-origin credentialed requests to any API endpoint and read authenticated responses containing user PII, email, admin status, and session-sensitive data. Commit 5e2b897ccac61eb6daca2dee4a6be3c4c2d93e13 contains a fix.	7.1	More Details
CVE-2026-40926	WWBN AVideo is an open source video platform. In versions 29.0 and prior, three admin-only JSON endpoints — `objects/categoryAddNew.json.php`, `objects/categoryDelete.json.php`, and `objects/pluginRunUpdateScript.json.php` — enforce only a role check (`Category::canCreateCategory()` / `User::isAdmin()`) and perform state-changing actions against the database without calling `isGlobalTokenValid()` or `forbidIfIsUntrustedRequest()`. Peer endpoints in the same directory (`pluginSwitch.json.php`, `pluginRunDatabaseScript.json.php`) do enforce the CSRF token, so the missing checks are an omission rather than a design choice. An attacker who lures a logged-in admin to a malicious page can create, update, or delete categories and force execution of any installed plugin's `updateScript()` method in the admin's session. Commit ee5615153c40628ab3ec6fe04962d1f92e67d3e2 contains a fix.	7.1	More Details
CVE-2026-41189	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, customer-thread editing is authorized through `ThreadPolicy::edit()`, which checks mailbox access but does not apply the assigned-only restriction from `ConversationPolicy`. A user who cannot view a conversation can still load and edit customer-authored threads inside it. Version 1.8.215 fixes the vulnerability.	7.1	More Details
CVE-2026-40090	Zarf is an Airgap Native Packager Manager for Kubernetes. Versions 0.23.0 through 0.74.1 contain an arbitrary file write vulnerability in the zarf package inspect sbom and zarf package inspect documentation subcommands. These subcommands output file paths are constructed by joining a user-controlled output directory with the package's Metadata.Name field read directly from the untrusted package's zarf.yaml manifest. Although Metadata.Name is validated against a regex on package creation, an attacker can unarchive a package to modify the Metadata.Name field to contain path traversal sequences such as ../../etc/cron.d/malicious or absolute paths like /home/user/.ssh/authorized_keys, along with the corresponding files inside SBOMS.tar. This allows writing attacker-controlled content to arbitrary filesystem locations within the permissions of the user running the inspect command. This issue has been fixed in version 0.74.2.	7.1	More Details
CVE-2026-6066	ConnectWise has released a security update for ConnectWise Automate™ that addresses a behavior in the ConnectWise Automate Solution Center where certain client-to-server communications could occur without transport-layer encryption. This could allow network-based interception of Solution Center traffic in Automate deployments. The issue has been resolved in Automate 2026.4 by enforcing secure communication for affected Solution Center connections.	7.1	More Details
CVE-2026-40591	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.214, the phone-conversation creation flow accepts attacker-controlled `customer_id`, `name`, `to_email`, and `phone` values and resolves the target customer in the backend without enforcing mailbox-scoped customer visibility. As a result, a low-privileged agent who can create a phone conversation in Mailbox A can bind the new Mailbox A phone conversation to a hidden customer from Mailbox B and add a new alias email to that hidden customer record by supplying `to_email`. Version 1.8.214 fixes the vulnerability.	7.1	More Details
CVE-2026-40518	ByteDance DeerFlow before commit 2176b2b contains a path traversal and arbitrary file write vulnerability in bootstrap-mode custom-agent creation where the agent name validation is bypassed. Attackers can supply traversal-style values or absolute paths as the agent name to influence directory creation and write files outside the intended custom-agent directory, potentially achieving arbitrary file write on the system subject to filesystem permissions.	7.1	More Details
CVE-2026-6421	A vulnerability has been found in Mobatek MobaXterm Home Edition up to 26.1. This affects an unknown part in the library msimg32.dll. The manipulation leads to uncontrolled search path. An attack has to be approached locally. The attack is considered to have high complexity. It is indicated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 26.2 is able to mitigate this issue. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	7.0	More Details
CVE-2026-41253	In iTerm2 through 3.6.9, displaying a .txt file can cause code execution via DCS 2000p and OSC 135 data, if the working directory contains a malicious file whose name is valid output from the conductor encoding path, such as a pathname with an initial ace/c+ substring, aka "hypothetical in-band signaling abuse." This occurs because iTerm2 accepts the SSH conductor protocol from terminal output that does not originate from a legitimate conductor session.	6.9	More Details
CVE-2026-41527	KDE Kleopatra before 26.08.0 on Windows allows local users to obtain the privileges of a Kleopatra user, because there is an error in the mechanism (KUniqueService) for ensuring that only one instance is running.	6.9	More Details
CVE-2026-39963	Serendipity is a PHP-powered weblog engine. In versions 2.6-beta2 and below, the serendipity_setCookie() function in include/functions_config.inc.php uses $_SERVER['HTTP_HOST'] without validation as the domain parameter of setcookie(). An attacker who can influence the Host header at login time, such as via MITM, reverse proxy misconfiguration, or load balancer manipulation, can force authentication cookies including session tokens and auto-login tokens to be scoped to an attacker-controlled domain. This enables session fixation, token leakage to attacker-controlled infrastructure, and privilege escalation if an admin logs in under a poisoned Host header. This issue has been fixed in version 2.6.0.	6.9	More Details
	OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Prior to 7.15.2, an authorization bypass		

CVE-2026-40574	exists in OAuth2 Proxy as part of the email_domain enforcement option. An attacker may be able to authenticate with an email claim such as attacker@evil.com@company.com and satisfy an allowed domain check for company.com, even though the claim is not a valid email address. The issue ONLY affects deployments that rely on email_domain restrictions and accept email claim values from identity providers or claim mappings that do not strictly enforce normal email syntax. This vulnerability is fixed in 7.15.2.	6.8	More Details
CVE-2026-34325	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Financial Services Analytical Applications Infrastructure executes to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 6.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H).	6.8	More Details
CVE-2026-40253	openCryptoki is a PKCS#11 library and provides tooling for Linux and AIX. In versions 3.26.0 and below, the BER/DER decoding functions in the shared common library (asn1.c) accept a raw pointer but no buffer length parameter, and trust attacker-controlled BER length fields without validating them against actual buffer boundaries. All primitive decoders are affected: ber_decode_INTEGER, ber_decode_SEQUENCE, ber_decode_OCTET_STRING, ber_decode_BIT_STRING, and ber_decode_CHOICE. Additionally, ber_decode_INTEGER can produce integer underflows when the encoded length is zero. An attacker supplying a malformed BER-encoded cryptographic object through PKCS#11 operations such as C_CreateObject or C_UnwrapKey, token loading from disk, or remote backend communication can trigger out-of-bounds reads. This affects all token backends (Soft, ICA, CCA, TPM, EP11, ICSF) since the vulnerable code is in the shared common library. A patch is available thorugh commit ed378f463ef73364c89feb0fc923f4dc867332a3.	6.8	More Details
CVE-2026-33220	Weblate is a web based localization tool. In versions prior to 5.17, the translation memory API exposed unintended endpoints, which in turn didn't perform proper access control. This issue has been fixed in version 5.17. If developers are unable to update immediately, they can disable this feature as the CDN add-on is not enabled by default.	6.8	More Details
CVE-2026-40284	WeGIA is a web manager for charitable institutions. In versions prior to 3.6.10, a Stored Cross-Site Scripting (XSS) vulnerability allows an authenticated user to inject malicious JavaScript via the "Destinatário" field. The payload is stored and later executed when viewing the dispatch page, impacting other users. Version 3.6.10 fixes the issue.	6.8	More Details
CVE-2026-40283	WeGIA is a web manager for charitable institutions. In versions prior to 3.6.10, a Stored Cross-Site Scripting (XSS) vulnerability allows an authenticated user to inject malicious JavaScript via the "Nome" field in the "Informações Pacientes" page. The payload is stored and executed when the patient information is viewed. Version 3.6.10 fixes the issue.	6.8	More Details
CVE-2026-40500	ProcessWire CMS version 3.0.255 and prior contain a server-side request forgery vulnerability in the admin panel's 'Add Module From URL' feature that allows authenticated administrators to supply arbitrary URLs to the module download parameter, causing the server to issue outbound HTTP requests to attacker-controlled internal or external hosts. Attackers can exploit differentiable error messages returned by the server to perform reliable internal network port scanning, host enumeration across RFC-1918 ranges, and potential access to cloud instance metadata endpoints.	6.8	More Details
CVE-2026-28741	Mattermost versions 10.11.x <= 10.11.12, 11.5.x <= 11.5.0, 11.4.x <= 11.4.2, 11.3.x <= 11.3.2 fail to validate CSRF tokens on an authentication endpoint which allows an attacker to update a user's authentication method via a CSRF attack by tricking a user into visiting a malicious page. Mattermost Advisory ID: MMSA-2026-00625	6.8	More Details
CVE-2026-40490	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. When redirect following is enabled (followRedirect(true)), versions of AsyncHttpClient prior to 3.0.9 and 2.14.5 forward Authorization and Proxy-Authorization headers along with Realm credentials to arbitrary redirect targets regardless of domain, scheme, or port changes. This leaks credentials on cross-domain redirects and HTTPS-to-HTTP downgrades. Additionally, even when stripAuthorizationOnRedirect is set to true, the Realm object containing plaintext credentials is still propagated to the redirect request, causing credential re-generation for Basic and Digest authentication schemes via NettyRequestFactory. An attacker who controls a redirect target (via open redirect, DNS rebinding, or MITM on HTTP) can capture Bearer tokens, Basic auth credentials, or any other Authorization header value. The fix in versions 3.0.9 and 2.14.5 automatically strips Authorization and Proxy-Authorization headers and clears Realm credentials whenever a redirect crosses origin boundaries (different scheme, host, or port) or downgrades from HTTPS to HTTP. For users unable to upgrade, set `(stripAuthorizationOnRedirect(true))` in the client config and avoid using Realm-based authentication with redirect following enabled. Note that `(stripAuthorizationOnRedirect(true))` alone is insufficient on versions prior to 3.0.9 and 2.14.5 because the Realm bypass still re-generates credentials. Alternatively, disable redirect following (`followRedirect(false)`) and handle redirects manually with origin validation.	6.8	More Details
CVE-2026-34314	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	6.8	More Details
CVE-2026-21709	A vulnerability allowing a local attacker with administrator privileges to bypass Windows Driver Signature Enforcement.	6.7	More Details
CVE-2026-1636	A potential DLL hijacking vulnerability was reported in Lenovo Service Bridge that, under certain conditions, could allow a local authenticated user to execute code with elevated privileges.	6.7	More Details

CVE-2026-26951	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a stack-based buffer overflow vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-35072	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command ('OS command injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-22761	Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-26942	Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-35153	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of argument delimiters in a command ('argument injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-35074	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-35073	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	6.7	More Details
CVE-2026-23779	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain root-level access.	6.7	More Details
CVE-2025-46641	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	6.6	More Details
CVE-2025-43937	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.6	More Details
CVE-2025-46607	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	6.6	More Details
CVE-2026-28684	python-dotenv reads key-value pairs from a .env file and can set them as environment variables. Prior to version 1.2.2, `set_key()` and `unset_key()` in python-dotenv follow symbolic links when rewriting `.env` files, allowing a local attacker to overwrite arbitrary files via a crafted symlink when a cross-device rename fallback is triggered. Users should upgrade to v.1.2.2 or, as a workaround, apply the patch manually.	6.6	More Details
CVE-2026-26274	October is a Content Management System (CMS) and web platform. Prior to 3.7.14 and 4.1.10, a vulnerability was identified in the Twig sandbox security policy that allowed database write operations when cms.safe_mode is enabled. Backend users with Developer permissions could use Twig template markup to execute insert, update, and delete operations on any database table through the query builder, which is included in the sandbox allow-list. This vulnerability is fixed in 3.7.14 and 4.1.10.	6.6	More Details
CVE-2026-34277	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Fluid Core). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L).	6.6	More Details
CVE-2026-20202	In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.6, 10.2.2510.10, 10.1.2507.20, 10.0.2503.13, and 9.3.2411.127, a user who holds a role that contains the high-privilege capability `edit_user`could create a specially crafted username that includes a null byte or a non-UTF-8 percent-encoded byte due to improper input validation. This could lead to inconsistent conversion of usernames into a proper format for storage and account management inconsistencies, such as being unable to edit or delete affected users.	6.6	More Details
CVE-2026-4135	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix, that during installation could allow a local authenticated user to perform an arbitrary file write with elevated privileges.	6.6	More Details

CVE-2026-39378	The nbconvert tool, jupyter nbconvert, converts Jupyter notebooks to various other formats via Jinja templates. In versions 6.5 through 7.17.0, when `HTMLExporter.embed_images=True`, nbconvert's markdown renderer allows arbitrary file read via path traversal in image references. A malicious notebook can exfiltrate sensitive files from the conversion host by embedding them as base64 data URIs in the output HTML. nbconvert 7.17.1 contains a fix. As a workaround, do not enable `HTMLExporter.embed_images`; it is not enabled by default.	6.5	More Details
CVE-2026-6588	A weakness has been identified in serge-chat serge up to 1.4TB. The impacted element is the function download_model/delete_model of the file api/src/serge/routers/model.py of the component Model API Endpoint. Executing a manipulation can lead to missing authentication. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2026-33569	Anviz CX2 Lite and CX7 administrative sessions occur over HTTP, enabling on-path attackers to sniff credentials and session data, which can be used to compromise the device.	6.5	More Details
CVE-2026-40587	blueprintUE is a tool to help Unreal Engine developers. Prior to 4.2.0, when a user changes their password via the profile edit page, or when a password reset is completed via the reset link, neither operation invalidates existing authenticated sessions for that user. A server-side session store associates userID → session; the current password change/reset flow updates only the password column in the users table and does not destroy or mark invalid any active sessions. As a result, an attacker who has already compromised a session retains full access to the account indefinitely — even after the legitimate user has detected the intrusion and changed their password — until the session's natural expiry time (configured as SESSION_GC_MAXLIFETIME, defaulting to 86400 seconds / 24 hours, with SESSION_LIFETIME=0 meaning persistent until browser close or GC, whichever is later). This vulnerability is fixed in 4.2.0.	6.5	More Details
CVE-2026-6579	A weakness has been identified in liangliangyy DjangoBlog up to 2.1.0.0. This impacts an unknown function of the file blog/views.py of the component Clean Endpoint. This manipulation causes missing authentication. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2026-22017	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-6755	Mitigation bypass in the DOM: postMessage component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	6.5	More Details
CVE-2026-40896	OpenProject is open-source, web-based project management software. Prior to version 17.3.0, a user with `manage_agendas` permission in any project can inject agenda items into meetings belonging to any other project on the instance — even projects they have no access to. No knowledge of the target project, meeting, or victim is required; the attacker can blindly spray items into every meeting on the instance by iterating sequential section IDs. Version 17.3.0 patches the issue.	6.5	More Details
CVE-2026-6770	Other issue in the Storage: IndexedDB component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	6.5	More Details
CVE-2026-40889	Frappe HR is an open-source human resources management solution (HRMS). Prior to versions 15.58.2 and 16.4.2, authenticated users can access unauthorized files by exploiting certain api endpoint. Versions 15.58.2 and 16.4.2 contain a patch. No known workarounds are available.	6.5	More Details
CVE-2026-32964	SD-330AC and AMC Manager provided by silex technology, Inc. contain an improper neutralization of CRLF sequences ('CRLF Injection') vulnerability. Processing some crafted configuration data may lead to arbitrary entries injected to the system configuration.	6.5	More Details
CVE-2026-32960	SD-330AC and AMC Manager provided by silex technology, Inc. contain an issue with a sensitive information in resource not removed before reuse. An attacker may login to the device without knowing the password by sending a crafted packet.	6.5	More Details
CVE-2026-32958	SD-330AC and AMC Manager provided by silex technology, Inc. use a hard-coded cryptographic key. An administrative user may be directed to apply a fake firmware update.	6.5	More Details
CVE-2026-6763	Mitigation bypass in the File Handling component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	6.5	More Details
CVE-2026-40907	WWBN AVideo is an open source video platform. In versions 29.0 and prior, the endpoint `plugin/Live/view/Live_restreams/list.json.php` contains an Insecure Direct Object Reference (IDOR) vulnerability that allows any authenticated user with streaming permission to retrieve other users' live restream configurations, including third-party platform stream keys and OAuth tokens (access_token, refresh_token) for services like YouTube Live, Facebook Live, and Twitch. Commit d5992fff2811df4adad1d9fc7d0a5837b882aed7 fixes the issue.	6.5	More Details
CVE-2025-66954	A vulnerability exists in the Buffalo Link Station version 1.85-0.01 that allows unauthenticated or guest-level users to enumerate valid usernames and their associated privilege roles. The issue is triggered by modifying a parameter within requests sent to the /nasapi endpoint.	6.5	More Details
CVE-2026-	Frappe HR is an open-source human resources management solution (HRMS). Prior to versions 15.54.0 and 14.38.1, a specially crafted request made to a certain endpoint could result in SQL injection, allowing an attacker to extract information	6.5	More Details

41320	they wouldn't otherwise be able to. Versions 15.54.0 and 14.38.1 contain a patch. No known workarounds are available.		
CVE-2026-1089	User-Controlled HTTP Header in Fortra's GoAnywhere MFT prior to version 7.10.0 allows attackers to trigger a DNS lookup, as well as DNS Rebinding and Information Disclosure.	6.5	More Details
CVE-2026-34276	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-34272	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-40491	gdown is a Google Drive public file/folder downloader. Versions prior to 5.2.2 are vulnerable to a Path Traversal attack within the extractall functionality. When extracting a maliciously crafted ZIP or TAR archive, the library fails to sanitize or validate the filenames of the archive members. This allow files to be written outside the intended destination directory, potentially leading to arbitrary file overwrite and Remote Code Execution (RCE). Version 5.2.2 contains a fix.	6.5	More Details
CVE-2026-41300	OpenClaw before 2026.3.31 contains a trust-decline vulnerability that preserves attacker-discovered endpoints in remote onboarding flows. Attackers can route gateway credentials to malicious endpoints by having their discovered URL survive the trust decline process into manual prompts requiring operator acceptance.	6.5	More Details
CVE-2026-34266	Vulnerability in the PeopleSoft Enterprise HCM Absence Management product of Oracle PeopleSoft (component: Absence Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Absence Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Absence Management accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Absence Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2026-39377	The nbconvert tool, jupyter nbconvert, converts Jupyter notebooks to various other formats via Jinja templates. Versions 6.5 through 7.17.0 allow arbitrary file writes to locations outside the intended output directory when processing notebooks containing crafted cell attachment filenames. The `ExtractAttachmentsPreprocessor` passes attachment filenames directly to the filesystem without sanitization, enabling path traversal attacks. This vulnerability provides complete control over both the destination path and file extension. Version 7.17.1 contains a patch.	6.5	More Details
CVE-2026-29647	In OpenXiangShan NEMU, insufficient Smstateen permission enforcement allows lower-privileged code to access IMSIC state via stopei/vstopei CSRs even when mstateen0.IMSIC is cleared, potentially enabling cross-context information leakage or disruption of interrupt handling.	6.5	More Details
CVE-2026-34271	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-22009	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-34270	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-25542	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. From 0.43.0 to 1.11.0, trusted resources verification policies match a resource source string (refSource.URI) against spec.resources[].pattern using regexp.MatchString. In Go, regexp.MatchString reports a match if the pattern matches anywhere in the string, so common unanchored patterns (including examples in tekton documentation) can be bypassed by attacker-controlled source strings that contain the trusted pattern as a substring. This can cause an unintended policy match and change which verification mode/keys apply.	6.5	More Details
CVE-2026-40293	OpenFGA is an authorization/permission engine built for developers. In versions 0.1.4 through 1.13.1, when OpenFGA is configured to use preshared-key authentication with the built-in playground enabled, the local server includes the preshared API key in the HTML response of the /playground endpoint. The /playground endpoint is enabled by default and does not require authentication. It is intended for local development and debugging and is not designed to be exposed to production environments. Only those who run OpenFGA with `--authn-method` preshared, with the playground enabled, and with the playground endpoint accessible beyond localhost or trusted networks are vulnerable. To remediate the issue, users should upgrade to OpenFGA v1.14.0, or disable the playground by running `./openfga run --playground-enabled=false.`	6.5	More Details
CVE-	The Plugin: CMS für Motorrad Werkstätten plugin for WordPress is vulnerable to SQL Injection via the 'arttype' parameter in all versions up to, and including, 1.0.0 due to insufficient escaping on the user supplied parameter and lack of sufficient		More

2026-6674	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	Details
CVE-2025-15470	The Eleganzo theme for WordPress is vulnerable to arbitrary directory deletion due to insufficient path validation in the akd_required_plugin_callback function in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary directories on the server, including the WordPress root directory.	6.5	More Details
CVE-2026-6764	Incorrect boundary conditions in the DOM: Device Interfaces component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	6.5	More Details
CVE-2026-3590	Mattermost versions 10.11.x <= 10.11.12, 11.5.x <= 11.5.0, 11.4.x <= 11.4.2, 11.3.x <= 11.3.2 fail to enforce atomic single-use consumption of guest magic link tokens, which allows an attacker with access to a valid magic link to establish multiple independent authenticated sessions via concurrent requests.. Mattermost Advisory ID: MMSA-2026-00624	6.5	More Details
CVE-2025-12141	In Grafana's alerting system, users with edit permissions for a contact point, specifically the permissions “alert.notifications:write” or “alert.notifications.receivers:test” that are granted as part of the fixed role "Contact Point Writer", which is part of the basic role Editor - can edit contact points created by other users, modify the endpoint URL to a controlled server. By invoking the test functionality, attackers can capture and extract redacted secure settings, such as authentication credentials for third-party services (e.g., Slack tokens). This leads to unauthorized access and potential compromise of external integrations.	6.5	More Details
CVE-2026-40458	PAC4J is vulnerable to Cross-Site Request Forgery (CSRF). A malicious attacker can craft a specially designed website which, when visited by a user, will automatically submit a forged cross-site request with a token whose hash collides with the victim's legitimate CSRF token. Importantly, the attacker does not need to know the victim’s CSRF token or its hash prior to the attack. Collisions in the deterministic String.hashCode() function can be computed directly, reducing the effective token's security space to 32 bits. This bypasses CSRF protection, allowing profile updates, password changes, account linking, and any other state-changing operations to be performed without the victim's consent. This issue was fixed in PAC4J versions 5.7.10 and 6.4.1	6.5	More Details
CVE-2026-40503	OpenHarness prior to commit dd1d235 contains a path traversal vulnerability that allows remote gateway users with chat access to read arbitrary files by supplying path traversal sequences to the /memory show slash command. Attackers can manipulate the path input parameter to escape the project memory directory and access sensitive files accessible to the OpenHarness process without filesystem containment validation.	6.5	More Details
CVE-2026-4666	The wpForo Forum plugin for WordPress is vulnerable to unauthorized modification of data due to the use of `extract($args, EXTR_OVERWRITE)` on user-controlled input in the `edit()` method of `classes/Posts.php` in all versions up to, and including, 2.4.16. The `post_edit` action handler in `Actions.php` passes `$_REQUEST['post']` directly to `Posts::edit()`, which calls `extract($args, EXTR_OVERWRITE)`. An attacker can inject `post[guestposting]=1` to overwrite the local `$guestposting` variable, causing the entire permission check block to be skipped. The nonce check uses a hardcoded `wpforo_verify_form` action shared across all 8 forum templates, so any user who can view any forum page obtains a valid nonce. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit the title, body, name, and email fields of any forum post, including posts in private forums, admin posts, and moderator posts. Content passes through `wpforo_kses()` which strips JavaScript but allows rich HTML.	6.5	More Details
CVE-2025-15636	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emarket-design YouTube Showcase allows Stored XSS.This issue affects YouTube Showcase: from n/a through 3.5.1.	6.5	More Details
CVE-2026-3861	LINE client for iOS versions prior to 26.3.0 contains a vulnerability in the in-app browser where opening a crafted web page can repeatedly trigger OS-level dialogs, potentially causing the iOS device to become temporarily inoperable.	6.5	More Details
CVE-2026-6080	The Tutor LMS plugin for WordPress is vulnerable to SQL Injection in versions up to and including 3.9.8. This is due to insufficient escaping on the 'date' parameter combined with direct interpolation into a SQL fragment before being passed to $wpdb->prepare(). This makes it possible for authenticated attackers with Admin-level access and above to append additional SQL queries and extract sensitive information from the database.	6.5	More Details
CVE-2026-34301	Vulnerability in the PeopleSoft Enterprise FIN Maintenance Management product of Oracle PeopleSoft (component: Work Order Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Maintenance Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Maintenance Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-34300	Vulnerability in the PeopleSoft Enterprise FIN Contracts product of Oracle PeopleSoft (component: Contracts). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Contracts. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Contracts accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-40910	frp is a fast reverse proxy. From 0.43.0 to 0.68.0, frp contains an authentication bypass in the HTTP vhost routing path when routeByHTTPUser is used as part of access control. In proxy-style requests, the routing logic uses the username from Proxy-Authorization to select the routeByHTTPUser backend, while the access control check uses credentials from the regular Authorization header. As a result, an attacker who can reach the HTTP vhost entrypoint and knows or can guess the protected routeByHTTPUser value may access a backend protected by httpUser / httpPassword even with an incorrect Proxy-Authorization password. This issue affects deployments that explicitly use routeByHTTPUser. It does not affect ordinary HTTP proxies that do not use this feature. This vulnerability is fixed in 0.68.1.	6.5	More Details

CVE-2026-20078	Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials. These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system.	6.5	More Details
CVE-2026-20081	Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials. These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system.	6.5	More Details
CVE-2026-34299	Vulnerability in the PeopleSoft Enterprise FIN Maintenance Management product of Oracle PeopleSoft (component: Work Order Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Maintenance Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Maintenance Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-3773	The Accessibility Suite by Ability, Inc plugin for WordPress is vulnerable to SQL Injection via the 'scan_id' parameter in all versions up to, and including, 4.20. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-22616	Eaton Intelligent Power Protector (IPP) software allows repeated authentication attempts against the web interface login page due to insufficient rate-limiting controls. This security issue has been fixed in the latest version of Eaton IPP which is available on the Eaton download centre.	6.5	More Details
CVE-2026-5758	JavaScript is vulnerable to prototype pollution in Mafintosh's protocol-buffers-schema Version 3.6.0, where an attacker may alter the application logic, bypass security checks, cause a DoS or achieve remote code execution.	6.5	More Details
CVE-2026-34295	Vulnerability in the PeopleSoft Enterprise SCM Purchasing product of Oracle PeopleSoft (component: Purchasing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM Purchasing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise SCM Purchasing accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-6364	Out of bounds read in Skia in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-6385	A flaw was found in FFmpeg. A remote attacker could exploit this vulnerability by providing a specially crafted MPEG-PS/VOB media file containing a malicious DVD subtitle stream. This vulnerability is caused by a signed integer overflow in the DVD subtitle parser's fragment reassembly bounds checks, leading to a heap out-of-bounds write. Successful exploitation can result in a denial of service (DoS) due to an application crash, and potentially lead to arbitrary code execution.	6.5	More Details
CVE-2026-25219	The `access_key` and `connection_string` connection properties were not marked as sensitive names in secrets masker. This means that user with read permission could see the values in Connection UI, as well as when Connection was accidentaly logged to logs, those values could be seen in the logs. Azure Service Bus used those properties to store sensitive values. Possibly other providers could be also affected if they used the same fields to store sensitive data. If you used Azure Service Bus connection with those values set or if you have other connections with those values storing sensitve values, you should upgrade Airflow to 3.1.8	6.5	More Details
CVE-2026-40924	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Prior to 1.11.1, the HTTP resolver's FetchHttpResource function calls io.ReadAll(resp.Body) with no response body size limit. Any tenant with permission to create TaskRuns or PipelineRuns that reference the HTTP resolver can point it at an attacker-controlled HTTP server that returns a very large response body within the 1-minute timeout window, causing the tekton-pipelines-resolvers pod to be OOM-killed by Kubernetes. Because all resolver types (Git, Hub, Bundle, Cluster, HTTP) run in the same pod, crashing this pod denies resolution service to the entire cluster. Repeated exploitation causes a sustained crash loop. The same vulnerable code path is reached by both the deprecated pkg/resolution/resolver/http and the current pkg/remoteresolution/resolver/http implementations. This vulnerability is fixed in 1.11.1.	6.5	More Details
CVE-2026-3488	The WP Statistics plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 14.16.4. This is due to missing capability checks on multiple AJAX handlers including `wp_statistics_get_filters`, `wp_statistics_getPrivacyStatus`, `wp_statistics_updatePrivacyStatus`, and `wp_statistics_dismiss_notices`. These endpoints only verify a `wp_rest` nonce via `check_ajax_referer()` but do not enforce any capability checks such as `current_user_can()` or the plugin's own `User::Access()` method. Since the `wp_rest` nonce is available to all authenticated WordPress users, this makes it possible for authenticated attackers, with Subscriber-level access and above, to access sensitive analytics data (user IDs, usernames, emails, visitor tracking data), retrieve and modify privacy audit compliance status, and dismiss administrative notices.	6.5	More Details
CVE-2026-40899	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a JDBC parameter blocklist bypass vulnerability in the MySQL datasource configuration. The Mysql class uses Lombok's @Data annotation, which auto-generates a public setter for the illegalParameters field that contains the JDBC security blocklist. When a datasource configuration is submitted as JSON, Jackson deserialization calls setIllegalParameters with an attacker-supplied empty list, replacing the blocklist before getJdbc() validation runs. This allows an authenticated attacker to include dangerous JDBC parameters such as allowLoadLocalInfile=true, and by pointing the datasource at a rogue MySQL server, exploit the LOAD DATA LOCAL INFILE protocol feature to read arbitrary files from the DataEase server filesystem, including sensitive	6.5	More Details

	environment variables and database credentials. This issue has been fixed in version 2.10.21.		
CVE-2026-6437	Improper neutralization of argument delimiters in the volume handling component in AWS EFS CSI Driver (aws-efs-csi-driver) before v3.0.1 allows remote authenticated users with PersistentVolume creation permissions to inject arbitrary mount options via comma injection. To remediate this issue, users should upgrade to version v3.0.1	6.5	More Details
CVE-2026-34308	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-40734	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zahlan Categories Images categories-images allows DOM-Based XSS.This issue affects Categories Images: from n/a through <= 3.3.1.	6.5	More Details
CVE-2026-34315	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N).	6.5	More Details
CVE-2026-34306	Vulnerability in the PeopleSoft Enterprise FIN Project Costing product of Oracle PeopleSoft (component: Projects). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Project Costing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Project Costing accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-34324	Vulnerability in the Oracle Life Sciences InForm product of Oracle Life Science Applications (component: App Server). Supported versions that are affected are 7.0.1.0 and 7.0.1.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences InForm. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Life Sciences InForm accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2026-34303	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-37100	An issue in the Bluetooth Low Energy (BLE) control interface of the Yamaha SR-B30A sound bar firmware 2.40 (Mobile App: Sound Bar Remote / version: 2.40) allows remote attackers within BLE radio range to connect without authentication via the Sound Bar Remote protocol	6.5	More Details
CVE-2026-34281	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	6.5	More Details
CVE-2026-34280	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Job Profile Manager). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2026-4817	The MasterStudy LMS WordPress Plugin for Online Courses and Education plugin for WordPress is vulnerable to Time-based Blind SQL Injection via the 'order' and 'orderby' parameters in the /lms/stm-lms/order/items REST API endpoint in versions up to and including 3.7.25. This is due to insufficient input sanitization combined with a design flaw in the custom Query builder class that allows unquoted SQL injection in ORDER BY clauses. When the Query builder detects parentheses in the sort_by parameter, it treats the value as a SQL function and directly concatenates it into the ORDER BY clause without any quoting. While esc_sql() is applied to escape quotes and backslashes, this cannot prevent ORDER BY injection when the values themselves are not wrapped in quotes in the resulting SQL statement. This makes it possible for authenticated attackers, with subscriber-level access and above, to append arbitrary SQL queries via the ORDER BY clause to extract sensitive information from the database including user credentials, session tokens, and other confidential data through time-based blind SQL injection techniques.	6.5	More Details
CVE-2026-34313	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
	WWBN AVideo is an open source video platform. In versions 29.0 and below, the directory traversal fix introduced in commit		

CVE-2026-41062	2375eb5e0 for `objects/aVideoEncoderReceiveImage.json.php` only checks the URL path component (via `parse_url($url, PHP_URL_PATH)`) for `..` sequences. However, the downstream function `try_get_contents_from_local()` in `objects/functionsFile.php` uses `explode('/videos/', $url)` on the **full URL string** including the query string. An attacker can place the `/videos/../../` traversal payload in the query string to bypass the security check and read arbitrary files from the server filesystem. Commit bd11c16ec894698e54e2cdae25026c61ad1ed441 contains an updated fix.	6.5	More Details
CVE-2026-5070	The Vantage theme for WordPress is vulnerable to Stored Cross-Site Scripting via Gallery block text content in versions up to, and including, 1.20.32 due to insufficient output escaping in the gallery template. 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-2026-3878	The WP Docs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdocs_options[icon_size]' parameter in all versions up to, and including, 2.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5162	The Royal Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Instagram Feed widget's 'instagram_follow_text' setting in all versions up to, and including, 1.7.1056 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-2026-1572	The Livemesh Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification of data and Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 9.0. This is due to missing authorization checks on the AJAX handler `lae_admin_ajax()` and insufficient output escaping on multiple checkbox settings fields. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in the plugin settings page that will execute whenever an administrator accesses the plugin settings page granted they can obtain a valid nonce, which can be leaked via the plugin's improper access control on settings pages.	6.4	More Details
CVE-2026-1559	The Youzify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'checkin_place_id' parameter in all versions up to, and including, 1.3.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13364	The WP Maps – Store Locator,Google Maps,OpenStreetMap,Mapbox,Listing,Directory & Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'put_wpgm' shortcode in all versions up to, and including, 4.8.7. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2840	The Email Encoder – Protect Email Addresses and Phone Numbers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eeb_mailto' shortcode in all versions up to, and including, 2.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4801	The Page Builder Gutenberg Blocks – CoBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via external iCal feed data in all versions up to, and including, 3.1.16 due to insufficient output escaping of event titles, descriptions, and locations fetched from external iCal feeds in the Events block rendering function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6048	The Flipbox Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Flipbox widget's button URL `custom_attributes` field in all versions up to, and including, 2.1.1 due to insufficient validation of custom attribute names. Specifically, the plugin uses `esc_html()` on the attribute name which does not prevent event handler attributes (e.g., `onmouseover`, `onclick`). 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-2026-3875	The BetterDocs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'betterdocs_feedback_form' shortcode in all versions up to, and including, 4.3.8. This is due to insufficient input sanitization and output escaping on user supplied shortcode attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0868	The EMC – Easily Embed Calendly Scheduling Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's calendly shortcode in all versions up to, and including, 4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2986	The Contextual Related Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'other_attributes' parameter in versions up to, and including, 4.2.1 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-2026-0894	The Content Blocks (Custom Post Widget) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's content_block shortcode in all versions up to, and including, 3.3.9 due to insufficient input sanitization and output escaping on user supplied values consumed from user-created content blocks. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3299	The WP YouTube Lyte plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'lyte' shortcode in all versions up to, and including, 1.7.29 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2026-3885	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'su_box' shortcode in all versions up to, and including, 7.4.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1354	Zero Motorcycles firmware versions 44 and prior enable an attacker to forcibly pair a device with the motorcycle via Bluetooth. Once paired, an attacker can utilize over-the-air firmware updating functionality to potentially upload malicious firmware to the motorcycle. The motorcycle must first be in Bluetooth pairing mode, and the attacker must be in proximity of the vehicle and understand the full pairing process, to be able to pair their device with the vehicle. The attacker's device must remain paired with and in proximity of the motorcycle for the entire duration of the firmware update.	6.4	More Details
CVE-2026-5717	The VI: Include Post By plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class_container' attribute of the 'include-post-by-cat' shortcode in all versions up to, and including, 0.4.200706 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3659	The WP Circliful plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the [circliful] shortcode and via multiple shortcode attributes of the [circliful_direct] shortcode in all versions up to and including 1.2. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, in the circliful_shortcode() function, the 'id' attribute value is concatenated directly into an HTML id attribute (line 285) without any escaping, allowing an attacker to break out of the double-quoted attribute and inject arbitrary HTML event handlers. Similarly, the circliful_direct_shortcode() function (line 257) outputs all shortcode attributes directly into HTML data-* attributes without escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3998	The WM JqMath plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'style' shortcode attribute of the [jqmath] shortcode in all versions up to and including 1.3. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. The generate_jqMathFormula() function directly concatenates the 'style' attribute value into an HTML style attribute without applying esc_attr() or any other escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4005	The Coachific Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'userhash' shortcode attribute in all versions up to and including 1.0. This is due to insufficient input sanitization and output escaping. The plugin uses sanitize_text_field() on the 'userhash' parameter, which strips HTML tags but does not escape characters significant in a JavaScript string context (such as double quotes, semicolons, and parentheses). The sanitized value is then directly interpolated into a JavaScript string within a <script> tag on line 29 without any JavaScript-specific escaping (e.g., wp_json_encode() or esc_js()). 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-2026-4011	The Power Charts Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the [pc] shortcode in all versions up to, and including, 0.1.0. This is due to insufficient input sanitization and output escaping on the 'id' shortcode attribute. Specifically, in the pc_shortcode() function, the 'id' attribute is extracted from user-supplied shortcode attributes and directly concatenated into an HTML div element's class attribute without any escaping or sanitization at line 62. The resulting HTML is then passed through html_entity_decode() before being returned, further undermining any potential safety. 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-2026-35252	Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: C Oracle SSL API). Supported versions that are affected are 12.2.1.4.0 and 12.1.3.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Security Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N).	6.4	More Details
CVE-2026-4852	The Image Source Control Lite – Show Image Credits and Captions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Image Source' attachment field in all versions up to, and including, 3.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2434	The Pz-LinkCard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'blogcard' shortcode attributes in all versions up to, and including, 2.5.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6799	A security flaw has been discovered in Comfast CF-N1-S 2.6.0.1. Affected by this issue is some unknown functionality of the file /cgi-bin/mbox-config?method=SET&section=ping_config of the component Endpoint. Performing a manipulation of the argument destination results in command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6829	nesquena hermes-webui contains a trust-boundary failure vulnerability that allows authenticated attackers to set or change a session workspace to an arbitrary existing directory on disk by manipulating workspace path parameters in endpoints such as /api/session/new, /api/session/update, /api/chat/start, and /api/workspaces/add. Attackers can repoint a session workspace to a directory outside the intended trusted root and then use ordinary file read and write APIs to access or modify files outside the intended workspace boundary within the permissions of the hermes-webui process.	6.3	More Details
CVE-	A security flaw has been discovered in TransformerOptimus SuperAGI up to 0.0.14. Affected by this vulnerability is the function get_project/update_project/get_projects_organisation of the file superagi/controllers/project.py. The manipulation		More

2026-6614	results in authorization bypass. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	Details
CVE-2026-31370	Honor E APP is affected by information leak vulnerability, successful exploitation of this vulnerability may affect service confidentiality.	6.3	More Details
CVE-2026-6613	A vulnerability was identified in TransformerOptimus SuperAGI up to 0.0.14. Affected is the function delete_agent/stop_schedule/get_schedule_data of the file superagi/controllers/agent.py. The manipulation of the argument agent_id leads to authorization bypass. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6612	A vulnerability was determined in TransformerOptimus SuperAGI up to 0.0.14. This impacts the function get_agent_execution/update_agent_execution of the file superagi/controllers/agent_execution.py of the component Agent Execution Endpoint. Executing a manipulation of the argument agent_execution_id can lead to authorization bypass. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6609	A flaw has been found in liangliangyy DjangoBlog up to 2.1.0.0. The affected element is the function form_valid of the file oauth/views.py. This manipulation of the argument oauthid causes improper authorization. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6571	A weakness has been identified in kodcloud KodExplorer up to 4.52. Affected by this vulnerability is the function roleGroupAction of the file /app/controller/systemRole.class.php. Executing a manipulation of the argument group_role can lead to authorization bypass. 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.	6.3	More Details
CVE-2026-6497	A vulnerability was determined in prasathmani TinyFileManager up to 2.6. Affected by this vulnerability is an unknown functionality of the file /filemanager.php?p= ajax=true&type=upload of the component File Upload Handler. This manipulation of the argument uploadurl causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-34323	Vulnerability in the Oracle Life Sciences InForm product of Oracle Life Science Applications (component: IDM Authentication). Supported versions that are affected are 7.0.1.0 and 7.0.1.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Life Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Life Sciences InForm. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L).	6.3	More Details
CVE-2026-6489	A security flaw has been discovered in QueryMine sms up to 7ab5a9ea196209611134525ffc18de25c57d9593. This issue affects some unknown processing of the file admin/addteacher.php of the component Background Management Page. The manipulation of the argument image results in unrestricted upload. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. 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.	6.3	More Details
CVE-2026-6599	A vulnerability was detected in langflow-ai langflow up to 1.8.3. The impacted element is the function get_client_ip/install_mcp_config of the file src/backend/base/langflow/api/v1/mcp_projects.py of the component Model Context Protocol Configuration API. Performing a manipulation of the argument X-Forwarded-For results in injection. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6573	A vulnerability was detected in PHPEMS 11.0. This affects the function temppage of the file /app/exam/controller/exams.master.php of the component Instant Exam Creation Handler. The manipulation of the argument uploadfile results in server-side request forgery. The attack can be executed remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-6576	A vulnerability was determined in liangliangyy DjangoBlog up to 2.1.0.0. The affected element is the function CommandHandler of the file servermanager/api/commonapi.py of the component WeChat Bot Interface. Executing a manipulation of the argument Source can lead to command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6744	A vulnerability was found in Bagisto up to 2.3.15. Affected is the function copy of the component Downloadable Link Handler. The manipulation results in server-side request forgery. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure and explains: "We already replied on the github advisories. All the security issues are addressed through security advisory. We will fix this in our upcomming releases."	6.3	More Details
CVE-2026-33145	xrdp is an open source RDP server. Versions through 0.10.5 allow an authenticated remote user to execute arbitrary commands on the server due to unsafe handling of the AlternateShell parameter in xrdp-sesman. When the AllowAlternateShell setting is enabled (which is the default when not explicitly configured), xrdp accepts a client-supplied AlternateShell value and executes it via /bin/sh -c during session initialization. This results in shell-interpreted execution of unsanitized, user-controlled input. This behavior effectively provides a scriptable remote command execution primitive over RDP within the security context of the authenticated user, occurring prior to normal window manager startup. This can bypass expected session initialization flows and operational assumptions that restrict execution to interactive desktop environments. This issue has been fixed in version 0.10.6.	6.3	More Details

CVE-2026-6649	A vulnerability was determined in Qibo CMS 1.0. Affected by this issue is some unknown functionality of the file /index/image/headers. Executing a manipulation of the argument starts can lead to server-side request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6587	A security flaw has been discovered in vibrantlabsai RAGAS up to 0.4.3. The affected element is the function _try_process_local_file/_try_process_url of the file src/ragas/metrics/collections/multi_modal_faithfulness/util.py of the component Collections Module. Performing a manipulation of the argument retrieved_contexts results in server-side request forgery. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The security patch for CVE-2025-45691 was applied to a different module only. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6616	A security vulnerability has been detected in TransformerOptimus SuperAGI up to 0.0.14. This affects the function extract_with_bs4/extract_with_3k/extract_with_lxml of the file superagi/helper/webpage_extractor.py of the component WebScraperTool. Such manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6586	A vulnerability was identified in TransformerOptimus SuperAGI up to 0.0.14. Impacted is the function get_budget/update_budget of the file superagi/controllers/budget.py of the component Budget Endpoint. Such manipulation leads to authorization bypass. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6626	A vulnerability was detected in Cockpit-HQ Cockpit up to 2.13.5. Affected by this issue is some unknown functionality of the component Asset Handler/Aggregate Handler. The manipulation results in improper neutralization of special elements in data query logic. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-35154	Dell PowerProtect Data Domain appliances, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper privilege management vulnerability in IDRAC. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges to access unauthorized delete operation in IDRAC.	6.3	More Details
CVE-2026-6729	HKUDS OpenHarness prior to PR #159 remediation contains a session key derivation vulnerability that allows authenticated participants in shared chats or threads to hijack other users' sessions by exploiting a shared ohmo session key that lacks sender identity verification. Attackers can reuse another user's conversation state and replace or interrupt their active tasks by colliding into the same session boundary through the shared chat or thread scope.	6.3	More Details
CVE-2026-31014	Dovestones Softwares AD Self Update <4.0.0.5 is vulnerable to Cross Site Request Forgery (CSRF). The affected endpoint processes state-changing requests without requiring a CSRF token or equivalent protection. The endpoint accepts application/x-www-form-urlencoded requests, and an originally POST-based request can be converted to a GET request while still successfully updating user details. This allows an attacker to craft a malicious request that, when visited by an authenticated user, can modify user account information without their consent.	6.3	More Details
CVE-2026-6628	A flaw has been found in phili67 Ecclesia CRM up to 8.0.0. This affects the function ValidateInput of the file /v2/query/view/ of the component Query Viewer Component. This manipulation of the argument custom causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6488	A vulnerability was identified in QueryMine sms up to 7ab5a9ea196209611134525ffc18de25c57d9593. This vulnerability affects unknown code of the file admin/editcourse.php of the component GET Request Parameter Handler. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might 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.	6.3	More Details
CVE-2026-35588	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.4, the Cassandra export module (`glances/exports/glances_cassandra/__init__.py`) interpolates `keyspace`, `table`, and `replication_factor` configuration values directly into CQL statements without validation. A user with write access to `glances.conf` can redirect all monitoring data to an attacker-controlled Cassandra keyspace. Version 4.5.4 contains a fix.	6.3	More Details
CVE-2026-6362	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted video file. (Chromium security severity: High)	6.3	More Details
CVE-2026-6620	A vulnerability was found in SonicCloudOrg sonic-server up to 2.0.0. The affected element is the function Upload of the file FileTool.java of the component File Upload Endpoint. The manipulation of the argument Type results in path traversal. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6618	A flaw has been found in langgenius dify up to 1.13.3. This issue affects the function parse_openai_plugin_json_to_tool_bundle of the file api/core/tools/utils/parser.py of the component ApiBasedToolSchemaParser. Executing a manipulation of the argument url can lead to server-side request forgery. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-6617	A vulnerability was detected in langgenius dify up to 0.6.9. This vulnerability affects the function get_api_tool_provider_remote_schema of the file api/services/tools/api_tools_manage_service.py of the component ApiToolManageService. Performing a manipulation of the argument url results in server-side request forgery. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2026-6634	A weakness has been identified in usememos memos up to 0.22.1. This affects the function memos_access_token of the file src/App.tsx of the component UpdateInstanceSetting. This manipulation of the argument additionalStyle/additionalScript causes improper authorization. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-40608	Next AI Draw.io is a next.js web application that integrates AI capabilities with draw.io diagrams. Prior to 0.4.15, the embedded HTTP sidecar contains three POST handlers (/api/state, /api/restore, and /api/history-svg) that process incoming requests by accumulating the entire request body into a JavaScript string without any size limitations. Node.js buffers the entire payload in the V8 heap. Sending a sufficiently large body (e.g., 500 MiB or more) will exhaust the process heap memory, leading to an Out-of-Memory (OOM) error that crashes the MCP server. This vulnerability is fixed in 0.4.15.	6.2	More Details
CVE-2025-46606	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper restriction of excessive authentication attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	6.2	More Details
CVE-2025-46605	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain a session fixation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	6.2	More Details
CVE-2026-41030	In ONLYOFFICE DesktopEditors before 9.3.0, the update service allows attackers to perform actions on files with SYSTEM privileges.	6.2	More Details
CVE-2026-5160	Versions of the package github.com/yuin/goldmark/renderer/html before 1.7.17 are vulnerable to Cross-site Scripting (XSS) due to improper ordering of URL validation and normalization. The renderer validates link destinations using a prefix-based check (IsDangerousURL) before resolving HTML entities. This allows an attacker to bypass protocol filtering by encoding dangerous schemes using HTML5 named character references. For example, a payload such as javascript:alert(1) is not recognized as dangerous during validation, leading to arbitrary script execution in the context of applications that render the URL.	6.1	More Details
CVE-2026-40919	A flaw was found in GIMP. This vulnerability, a buffer overflow in the `file-seattle-filmworks` plugin, can be exploited when a user opens a specially crafted Seattle Filmworks file. A remote attacker could leverage this to cause a denial of service (DoS), leading to the plugin crashing and potentially impacting the stability of the GIMP application.	6.1	More Details
CVE-2026-33812	Parsing a malicious font file can cause excessive memory allocation.	6.1	More Details
CVE-2026-4032	The CodeColorer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter in 'cc' comment shortcode in versions up to, and including, 0.10.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires comments to be enabled on the target post and guest comments to be allowed.	6.1	More Details
CVE-2025-6024	The authentication endpoint fails to encode user-supplied input before rendering it in the web page, allowing for script injection. An attacker can leverage this by injecting malicious scripts into the authentication endpoint. This can result in the user's browser being redirected to a malicious website, manipulation of the web page's user interface, or the retrieval of information from the browser. However, session hijacking is not possible due to the httpOnly flag protecting session-related cookies.	6.1	More Details
CVE-2026-4091	The OPEN-BRAIN plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.5.0. This is due to missing nonce verification on the settings form in the func_page_main() function. This makes it possible for unauthenticated attackers to inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-20170	A vulnerability in the Desktop Agent functionality of Cisco Webex Contact Center could have allowed an unauthenticated, remote attacker to conduct cross-site scripting attacks. Cisco has addressed this vulnerability in the Cisco Webex Contact Center service, and no customer action is needed. This vulnerability existed because HTML and script content was not properly handled. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to steal sensitive information from the browser, including authentication and session information.	6.1	More Details
CVE-2026-40565	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, FreeScout's linkify() function in app/Misc/Helper.php converts plain-text URLs in email bodies into HTML anchor tags without escaping double-quote characters (") in the URL. HTMLPurifier (called first via getCleanBody()) preserves literal " characters in text nodes. linkify() then wraps URLs including those " chars inside an unescaped href="..." attribute, breaking out of the href and injecting arbitrary HTML attributes. Version 1.8.213 fixes the issue.	6.1	More Details
CVE-2026-1852	The Product Pricing Table by WooBeWoo plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the updateLabel() and remove() functions. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages or delete pricing tables via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-10242	The authentication endpoint fails to adequately validate user-supplied input before reflecting it back in the response. This allows an attacker to inject malicious script payloads into the input parameters, which are then executed by the victim's browser. Successful exploitation can enable an attacker to redirect the user's browser to a malicious website, modify the UI of the web page, or retrieve information from the browser. However, the impact is limited as session-related sensitive cookies are protected by the httpOnly flag, preventing session hijacking.	6.1	More Details
CVE-2026-6711	The Website LLMs.txt plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 8.2.6. This is due to the use of filter_input() without a sanitization filter and insufficient output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can	6.1	More Details

	successfully trick an administrator into performing an action such as clicking on a link.		
CVE-2026-31013	Dovestones Softwares ADPhonebook <4.0.1.1 has a reflected cross-site scripting (XSS) vulnerability in the search parameter of the /ADPhonebook?Department=HR endpoint. User-supplied input is reflected in the HTTP response without proper input validation or output encoding, allowing execution of arbitrary JavaScript in the victim's browser.	6.1	More Details
CVE-2026-20059	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2026-40186	ApostropheCMS is an open-source Node.js content management system. A regression introduced in commit 49d0bb7, included in versions 2.17.1 of the ApostropheCMS-maintained sanitize-html package bypasses allowedTags enforcement for text inside nonTextTagsArray elements (textarea and option). ApostropheCMS version 4.28.0 is affected through its dependency on the vulnerable sanitize-html version. The code at packages/sanitize-html/index.js:569-573 incorrectly assumes that htmlparser2 does not decode entities inside these elements and skips escaping, but htmlparser2 10.x does decode entities before passing text to the ontext callback. As a result, entity-encoded HTML is decoded by the parser and then written directly to the output as literal HTML characters, completely bypassing the allowedTags filter. An attacker can inject arbitrary tags including XSS payloads through any allowed option or textarea element using entity encoding. This affects non-default configurations where option or textarea are included in allowedTags, which is common in form builders and CMS platforms. This issue has been fixed in version 2.17.2 of sanitize-html and 4.29.0 of ApostropheCMS.	6.1	More Details
CVE-2026-3355	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘crsearch’ parameter in all versions up to, and including, 5.101.0 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-2026-34283	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: Identity Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Identity Manager accessible data as well as unauthorized read access to a subset of Oracle Identity Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-1838	The Hostel plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcode_id' parameter in all versions up to, and including, 1.1.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-40302	zrok is software for sharing web services, files, and network resources. Prior to version 2.0.1, the proxyUi template engine uses Go's text/template (which performs no HTML escaping) instead of html/template. The GitHub OAuth callback handlers in both publicProxy and dynamicProxy embed the attacker-controlled refreshInterval query parameter verbatim into an error message when time.ParseDuration fails, and render that error unescaped into HTML. An attacker can deliver a crafted login URL to a victim; after the victim completes the GitHub OAuth flow, the callback page executes arbitrary JavaScript in the OAuth server's origin. Version 2.0.1 patches the issue.	6.1	More Details
CVE-2026-34269	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-34274	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Configurator accessible data as well as unauthorized read access to a subset of Oracle Configurator accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-40333	libgphoto2 is a camera access and control library. In versions up to and including 2.5.33, two functions in camlibs/ptp2/ptp-pack.c accept a data pointer but no length parameter, performing unbounded reads. Their callers in ptp_unpack_EOS_events() have xsize available but never pass it, leaving both functions unable to validate reads against the actual buffer boundary. Commit 1817ecead20c2aafa7549dac9619fe38f47b2f53 patches the issue.	6.1	More Details
CVE-2026-34284	Vulnerability in the Oracle Business Process Management Suite product of Oracle Fusion Middleware (component: Human workflow 11g+). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Process Management Suite accessible data as well as unauthorized read access to a subset of Oracle Business Process Management Suite accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE-2026-40340	libgphoto2 is a camera access and control library. Versions up to and including 2.5.33 have an out-of-bounds read vulnerability in `ptp_unpack_OI()` in `camlibs/ptp2/ptp-pack.c` (lines 530–563). The function validates `len < PTP_oi_SequenceNumber` (i.e., len < 48) but subsequently accesses offsets 48–56, up to 9 bytes beyond the validated boundary, via the Samsung Galaxy 64-bit objectsize detection heuristic. Commit 7c7f515bc88c3d0c4098ac965d313518e0ccbe33 fixes the issue.	6.1	More Details
CVE-2026-40255	AdonisJS HTTP Server is a package for handling HTTP requests in the AdonisJS framework. In @adonisjs/http-server versions prior to 7.8.1 and 8.0.0-next.0 through 8.1.3, and @adonisjs/core versions prior to 7.4.0, the response.redirect().back() method reads the Referer header from the incoming HTTP request and redirects to that URL without validating the host.An attacker who can influence the Referer header can cause the application to redirect users to a malicious external site. This affects all AdonisJS applications that use response.redirect().back() or response.redirect('back'). This issue has been fixed in versions 7.8.1 and 8.2.0 and 7.4.0 of @adonisjs/core.	6.1	More Details
CVE-2026-20136	A vulnerability in the CLI of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, local attacker with administrative privileges to perform a command injection attack on the underlying operating system and elevate privileges to root. This vulnerability is due to insufficient validation of user supplied input. An attacker could exploit this vulnerability by providing crafted input to a specific CLI command. A successful exploit could allow the attacker to elevate their privileges to root on the underlying operating system.	6.0	More Details
CVE-2026-35247	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2026-22615	Due to improper input validation in one of the Eaton Intelligent Power Protector (IPP) XML, it is possible for an attacker with admin privileges and access to the local system to inject malicious code resulting in arbitrary command execution. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download centre.	6.0	More Details
CVE-2026-22003	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u481 and 8u481-b50; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 6.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:H).	6.0	More Details
CVE-2025-12624	Active access tokens are not revoked or invalidated when a user account is locked within WSO2 Identity Server. This failure to enforce revocation allows previously issued, valid tokens to remain usable, enabling continued access to protected resources by locked user accounts. The security consequence is that a locked user account can maintain access to protected resources through the use of existing, unexpired access tokens. This creates a security gap where access control policies are bypassed, potentially leading to unauthorized data access or actions until the tokens naturally expire.	6.0	More Details
CVE-2026-40091	SpiceDB is an open source database system for creating and managing security-critical application permissions. In versions 1.49.0 through 1.51.0, when SpiceDB starts with log level info, the startup "configuration" log will include the full datastore DSN, including the plaintext password, inside DatastoreConfig.URI. This issue has been fixed in version 1.51.1. If users are unable to immediately upgrade, they can work around this issue by changing the log level to warn or error.	6.0	More Details
CVE-2026-40592	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.214, the undo-send route `GET /conversation/undo-reply/{thread_id}` checks only whether the current user can view the parent conversation. It does not verify that the current user created the reply being undone. In a shared mailbox, one agent can therefore recall another agent's just-sent reply during the 15-second undo window. Version 1.8.214 fixes the vulnerability.	5.9	More Details
CVE-2026-41245	Junrar is an open source java RAR archive library. Prior to version 7.5.10, a path traversal vulnerability in `LocalFolderExtractor` allows an attacker to write arbitrary files with attacker-controlled content into sibling directories when a crafted RAR archive is extracted. Version 7.5.10 fixes the issue.	5.9	More Details
CVE-2026-40265	Note Mark is an open-source note-taking application. In versions 0.19.1 and prior, the asset download endpoint at /api/notes/{noteID}/assets/{assetID} is registered without authentication middleware, and the backend query does not verify ownership or book visibility. An unauthenticated user who knows a valid note ID and asset ID can retrieve the full contents of private note assets without authentication, regardless of whether the associated book is public or private. This issue has been fixed in version 0.19.2.	5.9	More Details
CVE-2026-34294	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Microsoft Active Directory). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized read access to a subset of Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:N).	5.9	More Details
CVE-2026-	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in	5.9	More Details

34289	unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).		
CVE-2026-34288	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	5.9	More Details
CVE-2026-28263	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a cross-site Scripting vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection.	5.9	More Details
CVE-2026-22618	A security misconfiguration was identified in Eaton Intelligent Power Protector (IPP), where an HTTP response header was set with an insecure attribute, potentially exposing users to web-based attacks. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download centre.	5.9	More Details
CVE-2026-6414	@fastify/static versions 8.0.0 through 9.1.0 decode percent-encoded path separators (%2F) before filesystem resolution, while Fastify's router treats them as literal characters. This mismatch allows attackers to bypass route-based middleware or guards that protect files served by @fastify/static. For example, a route guard on a protected path can be circumvented by encoding the path separator in the URL. Upgrade to @fastify/static 9.1.1 to fix this issue. There are no workarounds.	5.9	More Details
CVE-2026-6370	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HashThemes Mini Ajax Cart for WooCommerce allows Stored XSS.This issue affects Mini Ajax Cart for WooCommerce: from n/a through 1.3.4.	5.9	More Details
CVE-2026-32959	SD-330AC and AMC Manager provided by silex technology, Inc. contain an issue with a use of a broken or risky cryptographic algorithm. Information in the traffic may be retrieved via man-in-the-middle attack.	5.9	More Details
CVE-2026-41389	OpenClaw versions 2026.4.7 before 2026.4.15 fail to enforce local-root containment on tool-result media paths, allowing arbitrary local and UNC file access. Attackers can craft malicious tool-result media references to trigger host-side file reads or Windows network path access, potentially disclosing sensitive files or exposing credentials.	5.8	More Details
CVE-2026-40567	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, an unauthenticated attacker can inject arbitrary HTML into outgoing emails generated by FreeScout by sending an email with a crafted From display name. The name is stored in the database without sanitization and rendered unescaped into outgoing reply emails via the `{%customer.fullName%}` signature variable. This allows embedding phishing links, tracking pixels, and spoofed content inside legitimate support emails sent from the organization's address. Version 1.8.213 fixes the issue.	5.8	More Details
CVE-2025-1241	Encrypted values in Fortra's GoAnywhere MFT prior to version 7.10.0 and GoAnywhere Agents prior to version 2.2.0 utilize a static IV which allows admin users to brute-force decryption of data.	5.8	More Details
CVE-2026-41153	In JetBrains Junie before 252.549.29 command execution was possible via malicious project file	5.8	More Details
CVE-2026-34318	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Shell accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	5.8	More Details
CVE-2026-25883	Vexa is an open-source, self-hostable meeting bot API and meeting transcription API. Prior to 0.10.0-260419-1910, the Vexa webhook feature allows authenticated users to configure an arbitrary URL that receives HTTP POST requests when meetings complete. The application performs no validation on the webhook URL, enabling Server-Side Request Forgery (SSRF). An authenticated attacker can set their webhook URL to target internal services (Redis, databases, admin panels), cloud metadata endpoints (AWS/GCP credential theft), and/or localhost services. Version 0.10.0-260419-1910 patches the issue.	5.8	More Details
CVE-2026-35241	Vulnerability in the PeopleSoft Enterprise CS Student Records product of Oracle PeopleSoft (component: Research Tracking). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Records. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Student Records accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).	5.7	More Details
CVE-2026-22617	Eaton Intelligent Power Protector (IPP) uses an insecure cookie configuration, which could allow a network-based attacker to intercept the cookie and exploit it through a man-in-the-middle attack. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download centre.	5.7	More Details
CVE-2026-40045	OpenClaw before 2026.4.2 accepts non-loopback cleartext ws:// gateway endpoints and transmits stored gateway credentials over unencrypted connections. Attackers can forge discovery results or craft setup codes to redirect clients to malicious endpoints, disclosing plaintext gateway credentials.	5.7	More Details
CVE-2026-35451	Twenty is an open source CRM. Prior to 1.20.6, a Stored Cross-Site Scripting (XSS) vulnerability exists in the BlockNote editor component. Due to a lack of protocol validation in the FileBlock component and insufficient server-side inspection of block content, an attacker can inject a javascript: URI into the url property of a file block. This allows the execution of arbitrary JavaScript when a user clicks on the malicious file attachment. This vulnerability is fixed in 1.20.6.	5.7	More Details

CVE-2026-6572	A security vulnerability has been detected in Collabora KodExplorer up to 4.52. Affected by this issue is some unknown functionality of the file /app/controller/share.class.php of the component fileUpload Endpoint. The manipulation of the argument fileUpload leads to improper authorization. Remote exploitation of the attack is possible. The attack's complexity is rated as high. The exploitation is known to be difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-40602	The Home Assistant Command-line interface (hass-cli) is a command-line tool for Home Assistant. Up to 1.0.0 of home-assitant-cli an unrestricted environment was used to handle Jninja2 templates instead of a sandboxed one. The user-supplied input within Jinja2 templates was rendered locally with no restrictions. This gave users access to Python's internals and extended the scope of templating beyond the intended usage. This vulnerability is fixed in 1.0.0.	5.6	More Details
CVE-2026-6578	A security flaw has been discovered in liangliangyy DjangoBlog up to 2.1.0.0. This affects an unknown function of the file djangoblog/settings.py of the component Setting Handler. The manipulation of the argument SECRET_KEY results in hard-coded credentials. The attack can be launched remotely. The attack requires a high level of complexity. The exploitability is reported as difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-39984	Sigstore Timestamp Authority is a service for issuing RFC 3161 timestamps. Versions 2.0.5 and below contain an authorization bypass vulnerability in the VerifyTimestampResponse function. VerifyTimestampResponse correctly verifies the certificate chain signature, but the TSA-specific constraint checks in VerifyLeafCert uses the first non-CA certificate from the PKCS#7 certificate bag instead of the leaf certificate from the verified chain. An attacker can exploit this by prepending a forged certificate to the certificate bag while the message is signed with an authorized key, causing the library to validate the signature against one certificate but perform authorization checks against another. This vulnerability only affects users of the timestamp-authority/v2/pkg/verification package and does not affect the timestamp-authority service itself or sigstore-go. The issue has been fixed in version 2.0.6.	5.5	More Details
CVE-2026-20161	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent could allow an authenticated, local attacker with low privileges to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are on the local file system of an affected device. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to bypass file system permissions and overwrite arbitrary files on the affected device.	5.5	More Details
CVE-2026-34302	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Loader). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Workflow. While the vulnerability is in Oracle Workflow, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Workflow accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Workflow. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:L).	5.5	More Details
CVE-2026-40915	A flaw was found in GIMP. A remote attacker could exploit an integer overflow vulnerability in the FITS image loader by providing a specially crafted FITS file. This integer overflow leads to a zero-byte memory allocation, which is then subjected to a heap buffer overflow when processing pixel data. Successful exploitation could result in a denial of service (DoS) or potentially arbitrary code execution.	5.5	More Details
CVE-2025-70795	STProcessMonitor 11.11.4.0, part of the Safetica Application suite, allows an admin-privileged user to send crafted IOCTL requests to terminate processes that are protected through a third-party implementation. This is caused by insufficient caller validation in the driver's IOCTL handler, enabling unauthorized processes to perform those actions in kernel space. Successful exploitation can lead to denial of service by disrupting critical third-party services or applications. Unauthorized processes load the driver and send a crafted IOCTL request (0xB822200C) to terminate processes protected by a third-party implementation. This action exploits insufficient caller validation in the driver's IOCTL handler, allowing unauthorized processes to perform termination operations in kernel space. Successful exploitation can lead to denial of service by disrupting critical third-party services or applications.	5.5	More Details
CVE-2026-40918	A flaw was found in GIMP. Processing a specially crafted PVR image file with large dimensions can lead to a denial of service (DoS). This occurs due to a stack-based buffer overflow and an out-of-bounds read in the PVR image loader, causing the application to crash. Systems that process untrusted PVR image files are affected.	5.5	More Details
CVE-2026-6245	A flaw was found in the System Security Services Daemon (SSSD). The pam_passkey_child_read_data() function within the PAM passkey responder fails to properly handle raw bytes received from a pipe. Because the data is treated as a NUL-terminated C string without explicit termination, it results in an out-of-bounds read when processed by functions like snprintf(). A local attacker could potentially trigger this vulnerability by initiating a crafted passkey authentication request, causing the SSSD PAM responder to crash, resulting in a local Denial of Service (DoS).	5.5	More Details
CVE-2026-40927	Docmost is open-source collaborative wiki and documentation software. Prior to 0.80.0, when leaving a comment on a page, it is possible to include a JavaScript URI as the link. When a user clicks on the link the JavaScript executes. This vulnerability is fixed in 0.80.0.	5.4	More Details
CVE-2026-22006	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Employee Snapshot). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain a stored cross-site scripting vulnerability in the @apostrophecms/color-field module, where color values prefixed with -- bypass TinyColor validation intended for CSS custom properties, and the launder.string() call performs only type coercion without stripping		

CVE-2026-33889	HTML metacharacters. These unsanitized values are then concatenated directly into <style> tags both in per-widget style elements rendered for all visitors and in the global stylesheet rendered for editors, with the output marked as safe HTML. An editor can inject a value which closes the style tag and executes arbitrary JavaScript in the browser of every visitor to any page containing the affected widget. This enables mass session hijacking, cookie theft, and privilege escalation to administrative control if an admin views draft content. This issue has been fixed in version 4.29.0.	5.4	More Details
CVE-2026-40483	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the Pledge Editor renders donation comment values directly into HTML input value attributes without escaping via htmlspecialchars(). An authenticated user with Finance permissions can inject HTML attribute-breaking characters and event handlers into the comment field, which are stored in the database and execute in the browser of any user who subsequently opens the pledge record for editing, resulting in stored XSS. This issue has been fixed in version 7.2.0.	5.4	More Details
CVE-2026-6383	A flaw was found in KubeVirt's Role-Based Access Control (RBAC) evaluation logic. The authorization mechanism improperly truncates subresource names, leading to incorrect permission evaluations. This allows authenticated users with specific custom roles to gain unauthorized access to subresources, potentially disclosing sensitive information or performing actions they are not permitted to do. Additionally, legitimate users may be denied access to resources.	5.4	More Details
CVE-2026-34429	Vvveb prior to 1.0.8.1 contains a stored cross-site scripting vulnerability that allows authenticated users with media upload and rename permissions to execute arbitrary JavaScript by bypassing MIME type validation and renaming uploaded files to executable extensions. Attackers can prepend a GIF89a header to HTML/JavaScript payloads to bypass upload validation, rename the file to .html extension, and execute malicious scripts in an administrator's browser session to create backdoor accounts and upload malicious plugins for remote code execution.	5.4	More Details
CVE-2026-41298	OpenClaw before 2026.4.2 fails to enforce write scopes on the POST /sessions/:sessionKey/kill endpoint in identity-bearing HTTP modes. Read-scoped callers can terminate running subagent sessions by sending requests to this endpoint, bypassing authorization controls.	5.4	More Details
CVE-2026-35232	Vulnerability in Oracle Fusion Middleware (component: Dynamic Monitoring Service). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Fusion Middleware. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Fusion Middleware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Fusion Middleware accessible data as well as unauthorized read access to a subset of Oracle Fusion Middleware accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2026-40479	Kimai is an open-source time tracking application. In versions 1.16.3 through 2.52.0, the escapeForHtml() function in KimaiEscape.js does not escape double quote or single quote characters. When a user's profile alias is inserted into an HTML attribute context via the team member form prototype and rendered through innerHTML, this incomplete escaping allows HTML attribute injection. An authenticated user with ROLE_USER privileges can store a malicious alias that executes JavaScript in the browser of any administrator viewing the team form, resulting in stored XSS with privilege escalation. This issue has been fixed in version 2.53.0.	5.4	More Details
CVE-2026-39112	Cross Site Scripting vulnerability in Apartment Visitors Management System Apartment Visitors Management System V1.1 in the visname parameter of visitors-form.php. An authenticated attacker can inject arbitrary JavaScript that is later executed when the malicious input is viewed in manage-newvisitors.php or visitor-detail.php.	5.4	More Details
CVE-2026-40923	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Prior to 1.11.1, a validation bypass in the VolumeMount path restriction allows mounting volumes under restricted /tekton/ internal paths by using .. path traversal components. The restriction check uses strings.HasPrefix without filepath.Clean, so a path like /tekton/home/../results passes validation but resolves to /tekton/results at runtime. This vulnerability is fixed in 1.11.1.	5.4	More Details
CVE-2026-22019	Vulnerability in the PeopleSoft Enterprise HCM Shared Components product of Oracle PeopleSoft (component: Person Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared Components. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Shared Components, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2026-39350	Istio is an open platform to connect, manage, and secure microservices. In versions 1.25.0 through 1.27.8, 1.28.0 through 1.28.5, 1.29.0, and 1.29.1, the serviceAccounts and notServiceAccounts fields in AuthorizationPolicy incorrectly interpret dots (.) as a regular expression matcher. Because . is a valid character in a service account name, an AuthorizationPolicy ALLOW rule targeting a service account such as cert-manager.io also matches cert-manager-io, cert-managerXio, etc. A DENY rule targeting the same name fails to block those variants. Fixes are available in versions 1.29.2, 1.28.6, and 1.27.9.	5.4	More Details
CVE-2026-6585	A vulnerability was determined in TransformerOptimus SuperAGI up to 0.0.14. This issue affects the function update_organisation of the file superagi/controllers/organisation.py of the component Organisation Update Endpoint. This manipulation of the argument organisation_id causes authorization bypass. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-40922	SiYuan is an open-source personal knowledge management system. In versions 3.6.1 through 3.6.3, a prior fix for XSS in bazaar README rendering (incomplete fix for CVE-2026-33066) enabled the Lute HTML sanitizer, but the sanitizer does not block iframe tags, and its URL-prefix blocklist does not effectively filter srcdoc attributes which contain raw HTML rather than URLs. A malicious bazaar package author can include an iframe with a srcdoc attribute containing embedded scripts in their README. When other users view the package in SiYuan's marketplace UI, the payload executes in the Electron context with full application privileges, enabling arbitrary code execution on the user's machine. This issue has been fixed in version 3.6.4.	5.4	More Details

CVE-2024-4867	The WSO2 API Manager developer portal accepts user-supplied input without enforcing expected validation constraints or proper output encoding. This deficiency allows a malicious actor to inject script content that is executed within the context of a user's browser. By leveraging this cross-site scripting vulnerability, a malicious actor can cause the browser to redirect to a malicious website, make changes to the UI of the web page, or retrieve information from the browser. However, session hijacking is not possible as all session-related sensitive cookies are protected by the httpOnly flag.	5.4	More Details
CVE-2026-40929	WWBN AVideo is an open source video platform. In versions 29.0 and prior, `objects/commentDelete.json.php` is a state-mutating JSON endpoint that deletes comments but performs no CSRF validation. It does not call `forbidIfIsUntrustedRequest()`, does not verify a CSRF/global token, and does not check `Origin`/`Referer`. Because AVideo intentionally sets `session.cookie_samesite=None` (to support cross-origin embed players), a cross-site request from any attacker-controlled page automatically carries the victim's `PHPSESSID`. Any authenticated victim who has authority to delete one or more comments (site moderators, video owners, and comment authors) can be tricked into deleting comments en masse simply by visiting an attacker page. Commit 184f36b1896f3364f864f17c1acca3dd8df3af27 contains a fix.	5.4	More Details
CVE-2026-2505	The Categories Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.3.1, via the 'z_taxonomy_image' shortcode. This is due to the shortcode rendering path passing attacker-controlled class input into a fallback image builder that concatenates HTML attributes without proper escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts that execute when users interact with the injected frontend page via the 'class' shortcode attribute.	5.4	More Details
CVE-2026-6496	A vulnerability was found in prasathmani TinyFileManager up to 2.6. Affected is an unknown function of the file /filemanager.php of the component POST Parameter Handler. The manipulation of the argument file[] results in path traversal. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-40948	The Keycloak authentication manager in `apache-airflow-providers-keycloak` did not generate or validate the OAuth 2.0 `state` parameter on the login / login-callback flow, and did not use PKCE. An attacker with a Keycloak account in the same realm could deliver a crafted callback URL to a victim's browser and cause the victim to be logged into the attacker's Airflow session (login-CSRF / session fixation), where any credentials the victim subsequently stored in Airflow Connections would be harvestable by the attacker. Users are advised to upgrade `apache-airflow-providers-keycloak` to 0.7.0 or later.	5.4	More Details
CVE-2026-41194	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, the mailbox OAuth disconnect action is implemented as `GET /mailbox/oauth-disconnect/{id}/{in_out}/{provider}`. It removes stored OAuth metadata from the mailbox and then redirects. Because it is a GET route, no CSRF token is required and the action can be triggered cross-site against a logged-in mailbox admin. Version 1.8.215 fixes the vulnerability.	5.4	More Details
CVE-2026-6774	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.4	More Details
CVE-2026-3369	The Better Find and Replace – AI-Powered Suggestions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via uploaded image title in versions up to, and including, 1.7.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-40928	WWBN AVideo is an open source video platform. In versions 29.0 and prior, multiple AVideo JSON endpoints under `objects/` accept state-changing requests via `$_REQUEST`/`$_GET` and persist changes tied to the caller's session user, without any anti-CSRF token, origin check, or referer check. A malicious page visited by a logged-in victim can silently cast/flip the victim's like/dislike on any comment (`objects/comments_like.json.php`), post a comment authored by the victim on any video, with attacker-chosen text (`objects/commentAddNew.json.php`), and/or delete assets from any category (`objects/categoryDeleteAssets.json.php`) when the victim has category management rights. Each endpoint is reachable from a browser via a simple `<img src="...">` tag or form submission, so exploitation only requires the victim to load an attacker-controlled HTML resource. Commit 7aaad601bd9cd7b993ba0ee1b1bea6c32ee7b77c contains a fix.	5.4	More Details
CVE-2026-34307	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Workflow). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2026-41061	WWBN AVideo is an open source video platform. In versions 29.0 and below, the `isValidDuration()` regex at `objects/video.php:918` uses `/^[0-9]{1,2}:[0-9]{1,2}:[0-9]{1,2}/` without a `$` end anchor, allowing arbitrary HTML/JavaScript to be appended after a valid duration prefix. The crafted duration is stored in the database and rendered without HTML escaping via `echo Video::getCleanDuration()` on trending pages, playlist pages, and video gallery thumbnails, resulting in stored cross-site scripting. Commit bcba324644df8b4ed1f891462455f1cd26822a45 contains a fix.	5.4	More Details
CVE-2026-41063	WWBN AVideo is an open source video platform. In versions 29.0 and below, an incomplete XSS fix in AVideo's `ParsedownSafeWithLinks` class overrides `inlineMarkup` for raw HTML but does not override `inlineLink()` or `inlineUrlTag()`, allowing `javascript:` URLs in markdown link syntax to bypass sanitization. Commit cae8f0dadbdd962c89b91d0095c76edb8aadcacf contains an updated fix.	5.4	More Details
CVE-2026-1509	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Arbitrary WordPress Action Execution in all versions up to, and including, 3.15.1. This is due to the plugin's `output_action_hook()` function accepting user-controlled input to trigger any registered WordPress action hook without proper authorization checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary WordPress action hooks via the Dynamic Data feature, potentially leading to privilege escalation, file inclusion, denial of service, or other security impacts depending on which action hooks are available in the WordPress installation.	5.4	More Details

CVE-2026-6583	A vulnerability has been found in TransformerOptimus SuperAGI up to 0.0.14. This affects the function delete_api_key/edit_api_key of the file superagi/controllers/api_key.py of the component API Key Management Endpoint. The manipulation leads to authorization bypass. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-6584	A vulnerability was found in TransformerOptimus SuperAGI up to 0.0.14. This vulnerability affects the function update_user of the file superagi/controllers/user.py of the component User Update Endpoint. The manipulation of the argument user_id results in authorization bypass. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-40155	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. In versions 4.12.0 through 4.17.1, simultaneous requests that trigger a nonce retry may cause the proxy cache fetcher to perform improper lookups for the token request results. Users are affected if their project uses both the vulnerable versions and the proxy handler /me/* and /my-org/* with DPoP enabled. This issue has been fixed in version 4.18.0.	5.4	More Details
CVE-2026-23756	GFI HelpDesk before 4.99.9 contains a stored cross-site scripting vulnerability in the Troubleshooter module where the subject POST parameter is not sanitized in Controller_Step.InsertSubmit() and EditSubmit() before being rendered by View_Step.RenderViewSteps(). An authenticated staff member can inject arbitrary JavaScript into the step subject field, and the payload executes when any user navigates to Troubleshooter > View Troubleshooter and clicks the affected step link.	5.4	More Details
CVE-2026-40740	Missing Authorization vulnerability in Themeum Tutor LMS tutor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through <= 3.9.7.	5.4	More Details
CVE-2026-23757	GFI HelpDesk before 4.99.10 contains a stored cross-site scripting vulnerability in the Reports module where the title parameter is passed directly to SWIFT_Report::Create() without HTML sanitization. Attackers can inject arbitrary JavaScript into the report title field when creating or editing a report, and the payload executes when staff members view and click the affected report link in the Manage Reports interface.	5.4	More Details
CVE-2026-6675	The Responsive Blocks – Page Builder for Blocks & Patterns plugin for WordPress is vulnerable to Unauthenticated Open Email Relay in all versions up to, and including, 2.2.0. This is due to insufficient authorization checks and missing server-side validation of the recipient email address supplied via a public REST API route. This makes it possible for unauthenticated attackers to send arbitrary emails to any recipient of their choosing through the affected WordPress site's mail server, effectively turning the site into an open mail relay.	5.3	More Details
CVE-2026-32648	Anviz CX2 Lite and CX7 are vulnerable to unauthenticated access that discloses debug configuration details (e.g., SSH/RTTY status), assisting attackers in reconnaissance against the device.	5.3	More Details
CVE-2026-3649	The Katalogportal PDF Sync plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.0.0. The katalogportal_popup_shortcode() function is registered as an AJAX handler via wp_ajax_katalogportal_shortcodePrinter but lacks any capability check (current_user_can()) or nonce verification. This allows any authenticated user, including Subscribers, to call the endpoint and retrieve a list of all synchronized PDF attachments (including those attached to private or draft posts) along with their titles, actual filenames, and the katalogportal_userid configuration value. The WP_Query uses post_status => 'any' which returns attachments regardless of the parent post's visibility status.	5.3	More Details
CVE-2026-40778	Missing Authorization vulnerability in Majestic Support Majestic Support majestic-support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Majestic Support: from n/a through <= 1.1.2.	5.3	More Details
CVE-2026-3642	The e-shot™ form builder plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.0.2. The eshot_form_builder_update_field_data() AJAX handler lacks any capability checks (current_user_can()) or nonce verification (check_ajax_referer()/wp_verify_nonce()). The function is registered via the wp_ajax_ hook, making it accessible to any authenticated user. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify form field configurations including mandatory status, field visibility, and form display preferences via the eshot_form_builder_update_field_data AJAX action.	5.3	More Details
CVE-2026-1782	The MetForm Pro plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 3.9.7 This is due to the payment integrations (Stripe/PayPal) trusting a user-submitted calculation field value without recomputing or validating it against the configured form price. This makes it possible for unauthenticated attackers to manipulate the payment amount via the 'mf-calculation' field in the form submission REST request granted there exists a specific form with this particular configuration.	5.3	More Details
CVE-2026-4812	The Advanced Custom Fields (ACF) plugin for WordPress is vulnerable to Missing Authorization to Arbitrary Post/Page Disclosure in versions up to and including 6.7.0. This is due to AJAX field query endpoints accepting user-supplied filter parameters that override field-configured restrictions without proper authorization checks. This makes it possible for unauthenticated attackers with access to a frontend ACF form to enumerate and disclose information about draft/private posts, restricted post types, and other data that should be restricted by field configuration.	5.3	More Details
CVE-2026-29644	XiangShan (open-source high-performance RISC-V processor) commit edb1dfaf7d290ae99724594507dc46c2c2125384 (2024-11-28) has improper gating of its distributed CSR write-enable path, allowing illegal CSR write attempts to alter custom PMA (Physical Memory Attribute) CSR state. Though the RISC-V privileged specification requires an illegal-instruction exception for non-existent/illegal CSR accesses, affected XiangShan versions may still propagate such writes to replicated PMA configuration state. Local attackers able to execute code on the core (privilege context depends on system integration) can exploit this to tamper with memory-attribute enforcement, potentially leading to privilege escalation, information disclosure, or denial of service depending on how PMA enforces platform security and isolation boundaries.	5.3	More Details
CVE-	Other issue in the Libraries component in NSS. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR		More

2026-6767	140.10, Thunderbird 150, and Thunderbird 140.10.	5.3	Details
CVE-2026-40935	WWBN AVideo is an open source video platform. In versions 29.0 and prior, `objects/getCaptcha.php` accepts the CAPTCHA length (`ql`) directly from the query string with no clamping or sanitization, letting any unauthenticated client force the server to generate a 1-character CAPTCHA word. Combined with a case-insensitive `strcasecmp` comparison over a ~33-character alphabet and the fact that failed validations do NOT consume the stored session token, an attacker can trivially brute-force the CAPTCHA on any endpoint that relies on `Captcha::validation()` (user registration, password recovery, contact form, etc.) in at most ~33 requests per session. Commit bf1c76989e6a9054be4f0eb009d68f0f2464b453 contains a fix.	5.3	More Details
CVE-2026-40763	Missing Authorization vulnerability in WP Royal Royal Elementor Addons royal-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Royal Elementor Addons: from n/a through <= 1.7.1056.	5.3	More Details
CVE-2026-1314	The 3D FlipBook – PDF Embedder, PDF Flipbook Viewer, Flipbook Image Gallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the send_post_pages_json() function in all versions up to, and including, 1.16.17. This makes it possible for unauthenticated attackers to retrieve flipbook page metadata for draft, private and password-protected flipbooks.	5.3	More Details
CVE-2026-21726	The CVE-2021-36156 fix validates the namespace parameter for path traversal sequences after a single URL decode, by double encoding, an attacker can read files at the Ruler API endpoint /loki/api/v1/rules/{namespace} Thanks to Prasanth Sundararajan for reporting this vulnerability.	5.3	More Details
CVE-2026-26399	A stack-use-after-return issue exists in the Arduino_Core_STM32 library prior to version 1.7.0. The pwm_start() function allocates a TIM_HandleTypeDef structure on the stack and passes its address to HAL initialization routines, where it is stored in a global timer handle registry. After the function returns, interrupt service routines may dereference this dangling pointer, resulting in memory corruption.	5.3	More Details
CVE-2026-40742	Missing Authorization vulnerability in Nelio Software Nelio AB Testing nelio-ab-testing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Nelio AB Testing: from n/a through <= 8.2.8.	5.3	More Details
CVE-2026-6765	Information disclosure in the Form Autofill component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	5.3	More Details
CVE-2026-34273	Vulnerability in Oracle GoldenGate (component: Libraries). Supported versions that are affected are 23.4-23.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GoldenGate. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GoldenGate accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2026-40304	zrok is software for sharing web services, files, and network resources. Prior to version 2.0.1, the unaccess handler (controller/unaccess.go) contains a logical error in its ownership guard: when a frontend record has environment_id = NULL (the marker for admin-created global frontends), the condition short-circuits to false and allows the deletion to proceed without any ownership verification. A non-admin user who knows a global frontend token can call DELETE /api/v2/unaccess with any of their own environment IDs and permanently delete the global frontend, taking down all public shares routed through it. Version 2.0.1 patches the issue.	5.3	More Details
CVE-2026-40737	Authorization Bypass Through User-Controlled Key vulnerability in VillaTheme COMPE compe-woo-compare-products allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects COMPE: from n/a through <= 1.1.4.	5.3	More Details
CVE-2026-6492	A vulnerability was detected in arnobt78 Hotel Booking Management System up to f8922d0e0f6ac1cc761974c7616f44c2bbc04bea. The impacted element is an unknown function of the file /api/health/detailed of the component Health Check Endpoint. Performing a manipulation results in information disclosure. Remote exploitation of the attack is possible. The exploit is now public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-22021	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2026-40730	Missing Authorization vulnerability in ThemeGrill ThemeGrill Demo Importer themegrill-demo-importer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ThemeGrill Demo Importer: from n/a through <= 2.0.0.6.	5.3	More Details
CVE-2026-6783	Incorrect boundary conditions, integer overflow in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.3	More Details
CVE-2026-	Other issue in the JavaScript Engine component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.3	More

6779			Details
CVE-2026-41301	OpenClaw versions 2026.3.22 before 2026.3.31 contain a signature verification bypass vulnerability in the Nostr DM ingress path that allows pairing challenges to be issued before event signature validation. An unauthenticated remote attacker can send forged direct messages to create pending pairing entries and trigger pairing-reply attempts, consuming shared pairing capacity and triggering bounded relay and logging work on the Nostr channel.	5.3	More Details
CVE-2026-6778	Invalid pointer in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.3	More Details
CVE-2025-31981	HCL BigFix Service Management (SM) Discovery is vulnerable to unenforced encryption due to port 80 (HTTP) being open, allowing unencrypted access. An attacker with access to the network traffic can sniff packets from the connection and uncover the data.	5.3	More Details
CVE-2026-6777	Other issue in the Networking: DNS component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.3	More Details
CVE-2026-22013	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.3	More Details
CVE-2026-41331	OpenClaw before 2026.3.31 contains a resource consumption vulnerability in Telegram audio preflight transcription that allows unauthorized group senders to trigger transcription processing. Attackers can exploit insufficient allowlist enforcement to cause resource or billing consumption by initiating audio preflight operations before authorization checks are applied.	5.3	More Details
CVE-2026-6775	Incorrect boundary conditions in the WebRTC component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	5.3	More Details
CVE-2026-6494	A flaw was found in the AAP MCP server. An unauthenticated remote attacker can exploit a log injection vulnerability by sending specially crafted input to the `toolsetroute` parameter. This parameter is not properly sanitized before being written to logs, allowing the attacker to inject control characters such as newlines and ANSI escape sequences. This enables the attacker to obscure legitimate log entries and insert forged ones, which could facilitate social engineering attacks, potentially leading to an operator executing dangerous commands or visiting malicious URLs.	5.3	More Details
CVE-2026-6491	A security vulnerability has been detected in libvips up to 8.18.2. The affected element is the function im_minpos_vec of the file libvips/deprecated/vips7compat.c of the component nip2 Handler. Such manipulation of the argument n leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The vendor confirms that they will "be removing the deprecated area in libvips 8.19".	5.3	More Details
CVE-2026-20152	A vulnerability in the authentication service feature of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass authentication policy requirements. This vulnerability is due to improper validation of user-supplied authentication input in HTTP requests. An attacker could exploit this vulnerability by sending HTTP requests that contain specific authentication requests to an affected device. A successful exploit could allow the attacker to bypass policy enforcement on the device. There is no direct impact to the Cisco Secure Web Appliance. However, as a result of exploiting this vulnerability, an attacker could send HTTP requests that should be restricted through the device.	5.3	More Details
CVE-2026-39886	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. Versions 3.4.0 through 3.4.9 have a signed integer overflow vulnerability in OpenEXR's HTJ2K (High-Throughput JPEG 2000) decompression path. The `ht_undo_impl()` function in `src/lib/OpenEXRCore/internal_ht.cpp` accumulates a bytes-per-line value (`bpl`) using a 32-bit signed integer with no overflow guard. A crafted EXR file with 16,385 FLOAT channels at the HTJ2K maximum width of 32,767 causes `bpl` to overflow `INT_MAX`, producing undefined behavior confirmed by UBSan. On an allocator-permissive host where the required ~64 GB allocation succeeds, the wrapped negative `bpl` value would subsequently be used as a per-scanline pointer advance, which would produce a heap out-of-bounds write. On a memory-constrained host, the allocation fails before `ht_undo_impl()` is entered. This is the second distinct integer overflow in `ht_undo_impl()`. CVE-2026-34545 addressed a different overflow in the same function — the `int16_t p` pixel-loop counter at line ~302 that overflows when iterating over channels whose `width` exceeds 32,767. The CVE-2026-34545 fix did not touch the `int bpl` accumulator at line 211, which is the subject of this advisory. The `bpl` accumulator was also not addressed by any of the 8 advisories in the 2026-04-05 v3.4.9 release batch. This finding is structurally identical to CVE-2026-34588 (PIZ `wcount*nx` overflow in `internal_piz.c`) and should be remediated with the same pattern. The CVE-2026-34588 fix did not touch `internal_ht.cpp`. Version 3.4.10 contains a remediation that addresses the vulnerability in `internal_ht.cpp`.	5.3	More Details
CVE-2026-	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain an authorization bypass vulnerability in the choices and counts query parameters of the REST API, where these query builders execute MongoDB distinct() operations that bypass the publicApiProjection restrictions intended to limit which fields are exposed publicly. The choices and counts parameters are processed via applyBuildersSafely before the projection is applied, and MongoDB's distinct operation does not respect projections, returning all distinct values directly. The results are returned in the API response without any filtering against publicApiProjection or removeForbiddenFields. An unauthenticated attacker can	5.3	More Details

39857	extract all distinct field values for any schema field type that has a registered query builder, including string, integer, float, select, boolean, date, slug, and relationship fields. Fields protected with viewPermission are similarly exposed, and the counts variant additionally reveals how many documents have each distinct value. Both the piece-type and page REST APIs are affected. This issue has been fixed in version 4.29.0.		
CVE-2026-40485	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the public API login endpoint (/api/public/user/login) returns distinguishable HTTP response codes based on whether a username exists: 404 for non-existent users and 401 for valid users with incorrect passwords. An unauthenticated attacker can exploit this difference to enumerate valid usernames, with no rate limiting or account lockout to impede the process. This issue has been fixed in version 7.2.0.	5.3	More Details
CVE-2026-5052	Vault's PKI engine's ACME validation did not reject local targets when issuing http-01 and tls-alpn-01 challenges. This may lead to these requests being sent to local network targets, potentially leading to information disclosure. Fixed in Vault Community Edition 2.0.0 and Vault Enterprise 2.0.0, 1.21.5, 1.20.10, and 1.19.16.	5.3	More Details
CVE-2026-33558	Information exposure vulnerability has been identified in Apache Kafka. The NetworkClient component will output entire requests and responses information in the DEBUG log level in the logs. By default, the log level is set to INFO level. If the DEBUG level is enabled, the sensitive information will be exposed via the requests and responses output log. The entire lists of impacted requests and responses are: * AlterConfigsRequest * AlterUserScramCredentialsRequest * ExpireDelegationTokenRequest * IncrementalAlterConfigsRequest * RenewDelegationTokenRequest * SaslAuthenticateRequest * createDelegationTokenResponse * describeDelegationTokenResponse * SaslAuthenticateResponse This issue affects Apache Kafka: from any version supported the listed API above through v3.9.1, v4.0.0. We advise the Kafka users to upgrade to v3.9.2, v4.0.1, or later to avoid this vulnerability.	5.3	More Details
CVE-2025-66335	Apache Doris MCP Server versions earlier than 0.6.1 are affected by an improper neutralization flaw in query context handling that may allow execution of unintended SQL statements and bypass of intended query validation and access restrictions through the MCP query execution interface. Version 0.6.1 and later are not affected.	5.3	More Details
CVE-2026-21999	Vulnerability in the XML Database component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise XML Database. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all XML Database accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	5.3	More Details
CVE-2026-3581	The Basic Google Maps Placemarks plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 1.10.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify stored map latitude and longitude options.	5.3	More Details
CVE-2026-3595	The Riaxe Product Customizer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.1.2. This is due to the plugin registering a REST API route at POST /wp-json/InkXEProductDesignerLite/customer/delete_customer without a permission_callback, causing WordPress to default to allowing unauthenticated access, and the inkxe_delete_customer() callback function taking an array of user IDs from the request body and passing each one directly to wp_delete_user() without any authentication or authorization checks. This makes it possible for unauthenticated attackers to delete arbitrary WordPress user accounts, including administrator accounts, leading to complete site lockout and data loss.	5.3	More Details
CVE-2026-5797	The Quiz And Survey Master plugin for WordPress is vulnerable to Arbitrary Shortcode Execution in versions up to and including 11.1.0. This is due to insufficient input sanitization and the execution of do_shortcode() on user-submitted quiz answer text. User-submitted answers pass through sanitize_text_field() and htmlspecialchars(), which only strip HTML tags but do not encode or remove shortcode brackets [and]. When quiz results are displayed, the plugin calls do_shortcode() on the entire results page output (including user answers), causing any injected shortcodes to be executed. This makes it possible for unauthenticated attackers to inject arbitrary WordPress shortcodes such as [qsm_result id=X] to access other users' quiz submissions without authorization, as the qsm_result shortcode lacks any authorization checks.	5.3	More Details
CVE-2026-35061	Anviz CX7 Firmware is vulnerable to the most recently captured test photo that can be retrieved without authentication, revealing sensitive operational imagery.	5.3	More Details
CVE-2026-5502	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized course content manipulation in versions up to and including 3.9.8. This is due to a missing authorization check in the tutor_update_course_content_order() function. The function only validates the nonce (CSRF protection) but does not verify whether the user has permission to manage course content. The can_user_manage() authorization check only executes when the 'content_parent' parameter is present in the request. When this parameter is omitted, the function proceeds directly to save_course_content_order() which manipulates the wp_posts table without any authorization validation. This makes it possible for authenticated attackers with subscriber-level access and above to detach all lessons from any topic, move lessons between topics, and modify the menu_order of course content, effectively allowing them to disrupt the structure of any course on the site.	5.3	More Details
CVE-2026-5427	The Kubio plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to and including 2.7.2. This is due to insufficient capability checks in the kubio_rest_pre_insert_import_assets() function, which is hooked to the rest_pre_insert_{post_type} filter for posts, pages, templates, and template parts. When a post is created or updated via the REST API, Kubio parses block attributes looking for URLs in the 'kubio' attribute namespace and automatically imports them via importRemoteFile() without verifying the user has the upload_files capability. This makes it possible for authenticated attackers with Contributor-level access and above to bypass WordPress's normal media upload restrictions and upload files fetched from external URLs to the media library, creating attachment posts in the database.	5.3	More Details
	The LatePoint plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.3.2. The vulnerability exists because the OsStripeConnectController::create_payment_intent_for_transaction action is registered as a public action (no authentication required) and loads invoices by sequential integer invoice_id without any		

CVE-2026-5234	access_key or ownership verification. This is in contrast to other invoice-related actions (view_by_key, payment_form, summary_before_payment) in OsInvoicesController which properly require a cryptographic UUID access_key. This makes it possible for unauthenticated attackers to enumerate valid invoice IDs via an error message oracle, create unauthorized transaction intent records in the database containing sensitive financial data (invoice_id, order_id, customer_id, charge_amount), and on sites with Stripe Connect configured, the response also leaks Stripe payment_intent_client_secret tokens, transaction_intent_key values, and payment amounts for any invoice.	5.3	More Details
CVE-2026-40908	WWBN AVideo is an open source video platform. In versions 29.0 and prior, the file `git.json.php` at the web root executes `git log -1` and returns the full output as JSON to any unauthenticated user. This exposes the exact deployed commit hash (enabling version fingerprinting against known CVEs), developer names and email addresses (PII), and commit messages which may contain references to internal systems or security fixes. As of time of publication, no known patched versions are available.	5.3	More Details
CVE-2026-24468	OpenAEV is an open source platform allowing organizations to plan, schedule and conduct cyber adversary simulation campaign and tests. Starting in version 1.11.0 and prior to version 2.0.13, the /api/reset endpoint behaves differently depending on whether the supplied username exists in the system. When a non-existent email is provided in the login parameter, the endpoint returns an HTTP 400 response (Bad Request). When a valid email is supplied, the endpoint responds with HTTP 200. This difference in server responses creates an observable discrepancy that allows an attacker to reliably determine which emails are registered in the application. By automating requests with a list of possible email addresses, an attacker can quickly build a list of valid accounts without any authentication. The endpoint should return a consistent response regardless of whether the username exists in order to prevent account enumeration. Version 2.0.13 fixes this issue.	5.3	More Details
CVE-2026-0718	The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites – PostX plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ultp_shareCount_callback() function in all versions up to, and including, 5.0.5. This makes it possible for unauthenticated attackers to modify the share_count post meta for any post, including private or draft posts.	5.3	More Details
CVE-2026-6608	A vulnerability was detected in lm-sys fastchat up to 0.2.36. Impacted is the function add_text of the component Arena Side-by-Side View Handler. The manipulation results in incorrect control flow. The attack can be launched remotely. The exploit is now public and may be used. The root cause was fixed in commit 34eca62 for gradio_block_arena_named.py, but three other files were missed.	5.3	More Details
CVE-2026-6607	A security vulnerability has been detected in lm-sys fastchat up to 0.2.36. This issue affects the function api_generate of the component Worker API Endpoint. The manipulation leads to resource consumption. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The identifier of the patch is c9e84b89c91d45191dc24466888de526fa04cf33. It is suggested to install a patch to address this issue. Commit ff66426 patched this issue in api_generate of base_model_worker.py and did miss other entry points.	5.3	More Details
CVE-2026-40249	free5GC is an open-source implementation of the 5G core network. In versions 4.2.1 and below of the UDR service, the PUT handler for updating Policy Data notification subscriptions at /nudr-dr/v2/policy-data/subs-to-notify/{subsId} does not return after request body retrieval or deserialization errors. Although HTTP 500 or 400 error responses are sent, execution continues and the processor is invoked with a potentially uninitialized or partially initialized PolicyDataSubscription object. This fail-open behavior may allow unintended modification of existing Policy Data notification subscriptions with invalid or empty input, depending on downstream processor and storage behavior. A patched version was not available at the time of publication.	5.3	More Details
CVE-2026-4160	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference via the 'submission_id' parameter in versions up to, and including, 6.1.21. This is due to missing authorization and ownership validation on a user controlled key in the Stripe SCA confirmation AJAX endpoint. This makes it possible for unauthenticated attackers to modify payment status of targeted pending submissions (for example, setting the status to "failed").	5.3	More Details
CVE-2026-32962	SD-330AC and AMC Manager provided by silex technology, Inc. contain a missing authentication for critical function issue. The device configuration may be altered without authentication.	5.3	More Details
CVE-2026-32961	SD-330AC and AMC Manager provided by silex technology, Inc. contain a heap-based buffer overflow vulnerability in packet data processing of sx_smpd. Processing a crafted packet may cause a temporary denial-of-service (DoS) condition.	5.3	More Details
CVE-2026-6410	@fastify/static versions 8.0.0 through 9.1.0 allow path traversal when directory listing is enabled via the list option. The dirList.path() function resolves directories outside the configured static root using path.join() without a containment check. A remote unauthenticated attacker can obtain directory listings for arbitrary directories accessible to the Node.js process, disclosing directory and file names. File contents are not disclosed. Upgrade to @fastify/static 9.1.1 to fix this issue. As a workaround, disable directory listing by removing the list option from the plugin configuration.	5.3	More Details
CVE-2026-32957	SD-330AC and AMC Manager provided by silex technology, Inc. contain a missing authentication for critical function issue on firmware maintenance. Arbitrary file may be uploaded on the device without authentication.	5.3	More Details
CVE-2026-24749	The Silverstripe Assets Module is a required component of Silverstripe Framework. In versions prior to 2.4.5 and 3.0.0-rc1 through 3.1.2, images rendered in templates or otherwise accessed via DBFile::getURL() or DBFile::getSourceURL() incorrectly add an access grant to the current session, which bypasses file permissions. This usually happens when creating an image variant, for example using a manipulation method like ScaleWidth() or Convert(). Note that if developers use DBFile directly in the $db configuration for a DataObject class that doesn't subclass File, and if they were setting the visibility of those files to "protected", those files will now need an explicit access grant to be accessed. If developers do not want to explicitly provide access grants for these files in their apps (i.e. they want these files to be accessible by default), they should use the "public" visibility. This issue has been fixed in versions 2.4.5 and 3.1.3.	5.3	More Details
CVE-2026-	Python-Multipart is a streaming multipart parser for Python. Versions prior to 0.0.26 have a denial of service vulnerability when parsing crafted `multipart/form-data` requests with large preamble or epilogue sections. Upgrade to version 0.0.26 or later, which skips ahead to the next boundary candidate when processing leading CR/LF data and immediately discards	5.3	More Details

40347	epilogue data after the closing boundary.		
CVE-2026-33093	Anviz CX7 Firmware is vulnerable to an unauthenticated POST to the device that captures a photo with the front facing camera, exposing visual information about the deployment environment.	5.3	More Details
CVE-2026-33888	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain an authorization bypass vulnerability in the getRestQuery method of the @apostrophecms/piece-type module, where the method checks whether a MongoDB projection has already been set before applying the admin-configured publicApiProjection. An unauthenticated attacker can supply a project query parameter in the REST API request, which is processed by applyBuildersSafely before the permission check, pre-populating the projection state and causing the publicApiProjection to be skipped entirely. This allows disclosure of any field on publicly queryable documents that the administrator explicitly restricted from the public API, such as internal notes, draft content, or metadata. Exploitation is trivial, requiring only appending query parameters to a public URL with no authentication. This issue has been fixed in version 4.29.0.	5.3	More Details
CVE-2026-40335	libgphoto2 is a camera access and control library. Versions up to and including 2.5.33 have an out-of-bounds read in `ptp_unpack_DPV()` in `camlibs/ptp2/ptp-pack.c` (lines 622–629). The UINT128 and INT128 cases advance `*offset += 16` without verifying that 16 bytes remain in the buffer. The entry check at line 609 only guarantees `*offset < total` (at least 1 byte available), leaving up to 15 bytes unvalidated. Commit 433bde9888d70aa726e32744cd751d7dbe94379a patches the issue.	5.2	More Details
CVE-2026-35244	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.24.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:N).	5.2	More Details
CVE-2026-40338	libgphoto2 is a camera access and control library. Versions up to and including 2.5.33 have an out-of-bounds read in the PTP_DPFF_Enumeration case of `ptp_unpack_Sony_DPD()` in `camlibs/ptp2/ptp-pack.c` (line 856). The function reads a 2-byte enumeration count N via `dtoh16o(data, *poffset)` without verifying that 2 bytes remain in the buffer. The standard `ptp_unpack_DPD()` at line 704 has this exact check, confirming the Sony variant omitted it by oversight. Commit 3b9f9696be76ae51dca983d9dd8ce586a2561845 fixes the issue.	5.2	More Details
CVE-2026-40339	libgphoto2 is a camera access and control library. Versions up to and including 2.5.33 have an out-of-bounds read in `ptp_unpack_Sony_DPD()` in `camlibs/ptp2/ptp-pack.c` (line 842). The function reads the FormFlag byte via `dtoh8o(data, *poffset)` without a prior bounds check. The standard `ptp_unpack_DPD()` at lines 686–687 correctly validates `*offset + sizeof(uint8_t) > dpdlen` before this same read, but the Sony variant omits this check entirely. Commit 09f8a940b1e418b5693f5c11e3016a1ad2cea62d fixes the issue.	5.2	More Details
CVE-2026-40337	The Sentry kernel is a high security level micro-kernel implementation made for high security embedded systems. A given task with one of the DEV or IO capability is able to interact with another task's IRQ line through the __sys_int_* syscall familly. Prior to version 0.4.7, this can lead to DoS and covert-channels between this task and the outer world. A patch is available in version 0.4.7. As a workaround, reduce tasks that have the DEV and IO capability to a single one.	5.1	More Details
CVE-2025-36579	Dell Client Platform BIOS contains a Weak Password Recovery Mechanism vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability, leading to unauthorized access.	5.1	More Details
CVE-2026-6654	Double-Free / Use-After-Free (UAF) in the `IntoIter::drop` and `ThinVec::clear` functions in the thin_vec crate. A panic in `ptr::drop_in_place` skips setting the length to zero.	5.1	More Details
CVE-2026-40917	A flaw was found in GIMP. This vulnerability, a heap buffer over-read in the `icns_slurp()` function, occurs when processing specially crafted ICNS image files. An attacker could provide a malicious ICNS file, potentially leading to application crashes or information disclosure on systems that process such files.	5.0	More Details
CVE-2026-41034	ONLYOFFICE DocumentServer before 9.3.0 has an untrusted pointer dereference in XLS processing/conversion (via pictFmla.cbBufInCtlStm and other vectors), leading to an information leak and ASLR bypass.	5.0	More Details
CVE-2026-34244	Weblate is a web based localization tool. In versions prior to 5.17, a user with the project.edit permission (granted by the per-project "Administration" role) can configure machine translation service URLs pointing to arbitrary internal network addresses. During configuration validation, Weblate makes an HTTP request to the attacker-controlled URL and reflects up to 200 characters of the response body back to the user in an error message. This constitutes a Server-Side Request Forgery (SSRF) with partial response read. This issue has been fixed in version 5.17. If developers are unable to immediately upgrade, they can limit available machinery services via WEBLATE_MACHINERY setting.	5.0	More Details
CVE-2026-40256	Weblate is a web based localization tool. In versions prior to 5.17, repository-boundary validation relies on string prefix checks on resolved absolute paths. In multiple code paths, the check uses startswith against the repository root path. This is not path-segment aware and can be bypassed when the external path shares the same string prefix as the repository path (for example, repo and repo_outside). This issue has been fixed in version 5.17.	5.0	More Details
CVE-2026-35248	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of	5.0	More Details

	Oracle VM VirtualBox. CVSS 3.1 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:L).		
CVE-2026-40002	Red Magic 11 Pro (NX809J) contains a vulnerability that allows non-privileged applications to trigger sensitive operations. The vulnerability stems from the lack of validation for applications accessing the service interface. Exploiting this vulnerability, an attacker can write files to specific partitions and set writable system properties.	5.0	More Details
CVE-2026-40916	A flaw was found in GIMP. A stack buffer overflow vulnerability in the TIM image loader's 4BPP decoding path allows a local user to cause a Denial of Service (DoS). By opening a specially crafted TIM image file, the application crashes due to an unconditional overflow when writing to a variable-length array.	5.0	More Details
CVE-2026-33440	Weblate is a web based localization tool. In versions prior to 5.17, the ALLOWED_ASSET_DOMAINS setting applied only to the first issued requests and didn't restrict possible redirects. This issue has been fixed in version 5.17.	5.0	More Details
CVE-2026-34319	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Shell. CVSS 3.1 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H).	5.0	More Details
CVE-2026-34317	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Core Client). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Shell executes to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Shell. CVSS 3.1 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H).	5.0	More Details
CVE-2026-22002	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-34293	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.45. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-35239	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-4853	The JetBackup – Backup, Restore & Migrate plugin for WordPress is vulnerable to Path Traversal leading to Arbitrary Directory Deletion in versions up to and including 3.1.19.8. This is due to insufficient input validation on the fileName parameter in the file upload handler. The plugin sanitizes the fileName parameter using sanitize_text_field(), which removes HTML tags but does not prevent path traversal sequences like '../'. The unsanitized filename is then directly concatenated in Upload::getFileLocation() without using basename() or validating the resolved path stays within the intended directory. When an invalid file is uploaded, the cleanup logic calls dirname() on the traversed path and passes it to Util::rm(), which recursively deletes the entire resolved directory. This makes it possible for authenticated attackers with administrator-level access to traverse outside the intended upload directory and trigger deletion of critical WordPress directories such as wp-content/plugins, effectively disabling all installed plugins and causing severe site disruption.	4.9	More Details
CVE-2026-25525	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 version 20.17.0, the Dataflow module in OpenMage LTS uses a weak blacklist filter (`str_replace('../', '', $input)`) to prevent path traversal attacks. This filter can be bypassed using patterns like `..././` or `..../`, which after the replacement still result in `../`. An authenticated administrator can exploit this to read arbitrary files from the server filesystem. Version 20.17.0 patches the issue.	4.9	More Details
CVE-2026-35238	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-35237	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-35236	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE-2026-26067	October is a Content Management System (CMS) and web platform. Prior to 3.7.14 and 4.1.10, a server-side information disclosure vulnerability was identified in the handling of CSS preprocessor files. Backend users with Editor permissions could craft .less, .sass, or .scss files that leverage the compiler's import functionality to read arbitrary files from the server. This worked even with cms.safe_mode enabled. This vulnerability is fixed in 3.7.14 and 4.1.10.	4.9	More Details
CVE-2026-35235	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-22004	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-21998	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-34304	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-22005	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-35240	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-35234	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-31927	Anviz CX7 Firmware is vulnerable to an authenticated CSV upload which allows path traversal to overwrite arbitrary files (e.g., /etc/shadow), enabling unauthorized SSH access when combined with debug-setting changes	4.9	More Details
CVE-2026-34267	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-3330	The Form Maker by 10Web plugin for WordPress is vulnerable to SQL Injection via the 'ip_search', 'startdate', 'enddate', 'username_search', and 'useremail_search' parameters in all versions up to, and including, 1.15.40. This is due to the `WDW_FM_Library::validate_data()` method calling `stripslashes()` on user input (removing WordPress's `wp_magic_quotes()` protection) and the `FMModelSubmissions_fm::get_labels_parameters()` function directly concatenating user-supplied values into SQL queries without using `$wpdb->prepare()`. 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. Additionally, the Submissions controller skips nonce verification for the `display` task, which means this vulnerability can be triggered via CSRF by tricking an administrator into clicking a crafted link.	4.9	More Details
CVE-2026-20148	A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system and read arbitrary files. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system.	4.9	More Details
CVE-2026-40962	FFmpeg before 8.1 has an integer overflow and resultant out-of-bounds write via CENC (Common Encryption) subsample data to libavformat/mov.c.	4.9	More Details
CVE-2026-	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.45. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	4.9	More

34278	hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		Details
CVE-2026-34164	Valtimo is an open-source business process automation platform. In versions 13.0.0 through 13.21.0, the InboxHandlingService logs the full content of every incoming inbox message at INFO level. Inbox messages can contain highly sensitive information including personal data (PII), citizen identifiers (BSN), and case details. This data is exposed to anyone with access to application logs or any Valtimo user with the admin role through the Admin UI logging module. This issue has been fixed in version 13.22.0. If developers are unable to upgrade immediately, they can restrict access to application logs and adjust the log level for com.ritense.inbox to WARN or higher in their application configuration as a workaround.	4.9	More Details
CVE-2026-22751	Vulnerability in Spring Spring Security. Applications that explicitly configure One-Time Token login with JdbcOneTimeTokenService are vulnerable to a Time-of-check Time-of-use (TOCTOU) race condition. This issue affects Spring Security: from 6.4.0 through 6.4.15, from 6.5.0 through 6.5.9, from 7.0.0 through 7.0.4.	4.8	More Details
CVE-2026-33472	Cryptomator is an open-source client-side encryption application for cloud storage. Version 1.19.1 contains a logic flaw in CheckHostTrustController.getAuthority() that allows an attacker to bypass the security fix for CVE-2026-32303. The method hardcodes the URI scheme based on port number, causing HTTPS URLs with port 80 to produce the same authority string as HTTP URLs, which defeats both the consistency check and the HTTP block validation. An attacker with write access to a cloud-synced vault.cryptomator file can craft a Hub configuration where apiBaseUrl and authEndpoint use HTTPS with port 80 to pass auto-trust validation, while tokenEndpoint uses plaintext HTTP. The vault is auto-trusted without user prompt, and a network-positioned attacker can intercept the OAuth token exchange to access the Cryptomator Hub API as the victim. This issue has been fixed in version 1.19.2.	4.8	More Details
CVE-2026-34321	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N).	4.8	More Details
CVE-2026-40606	mitmproxy is a interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers and mitmweb is a web-based interface for mitmproxy. In mitmproxy 12.2.1 and below, the builtin LDAP proxy authentication does not correctly sanitize the username when querying the LDAP server. This allows a malicious client to bypass authentication. Only mitmproxy instances using the proxyauth option with LDAP are affected. This option is not enabled by default. The vulnerability has been fixed in mitmproxy 12.2.2 and above.	4.8	More Details
CVE-2026-20132	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative write privileges to conduct a stored cross-site scripting (XSS) attack or a reflected XSS attack against a user of the web-based management interface of an affected device. These vulnerabilities are due to insufficient sanitization of user-supplied data that is stored in the web page. An attacker could exploit these vulnerabilities by convincing a user of the interface to click a specific link or view an affected web page. The injected script code may be executed in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	4.8	More Details
CVE-2026-23753	GFI HelpDesk before 4.99.9 contains a stored cross-site scripting vulnerability in the language management functionality where the charset POST parameter is passed directly to SWIFT_Language::Create() without HTML sanitization and subsequently rendered unsanitized by View_Language.RenderGrid(). An authenticated administrator can inject arbitrary JavaScript through the charset field when creating or editing a language, and the payload executes in the browser of any administrator viewing the Languages page.	4.8	More Details
CVE-2026-23752	GFI HelpDesk before 4.99.9 contains a stored cross-site scripting vulnerability in the template group creation and editing functionality that allows authenticated administrators to inject arbitrary JavaScript by manipulating the companyname POST parameter without HTML sanitization. Attackers can inject malicious scripts through the companyname field that execute in the browsers of any administrator viewing the Templates > Groups page.	4.8	More Details
CVE-2026-40593	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the User Editor (UserEditor.php) renders stored usernames directly into an HTML input value attribute without applying htmlspecialchars(). An administrator can save a username containing HTML attribute-breaking characters and event handlers, which execute in the browser of any administrator who subsequently views that user's editor page, resulting in stored XSS. This issue has been fixed in version 7.2.0.	4.8	More Details
CVE-2026-40594	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev98, the set_session_cookie_secure before_request handler in src/pyload/webui/app/__init__.py reads the X-Forwarded-Proto header from any HTTP request without validating that the request originates from a trusted proxy, then mutates the global Flask configuration SESSION_COOKIE_SECURE on every request. Because pyLoad uses the multi-threaded Cheroot WSGI server (request_queue_size=512), this creates a race condition where an attacker's request can influence the Secure flag on other users' session cookies — either downgrading cookie security behind a TLS proxy or causing a session denial-of-service on plain HTTP deployments. This vulnerability is fixed in 0.5.0b3.dev98.	4.8	More Details
CVE-2026-5721	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 6.5.0.4. This is due to insufficient input sanitization and output escaping in the prepareCellOutput() method of the LinkWDTColumn, ImageWDTColumn, and EmailWDTColumn classes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, given that they can trick an Administrator into importing data from an attacker-controlled source and the affected column types (Link, Image, or Email) are configured.	4.7	More Details
CVE-2026-	Cryptographic algorithm downgrade in the caching layer of Amazon AWS Encryption SDK for Python before version 3.3.1 and before version 4.0.5 might allow an authenticated local threat actor to bypass key commitment policy enforcement via a shared key cache, resulting in ciphertext that can be decrypted to multiple different plaintexts. To remediate this issue, users	4.7	More Details

6550	should upgrade to version 3.3.1, 4.0.5 or above.		
CVE-2026-6650	A vulnerability was identified in Z-BlogPHP 1.7.5. This affects the function App::UnPack of the file /zb_users/plugin/AppCentre/app_upload.php of the component ZBA File Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-6561	A vulnerability was detected in EyouCMS up to 1.7.1. This issue affects the function edit_adminlogo of the file application/admin/controller/Index.php. Performing a manipulation of the argument filename results in unrestricted upload. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-34298	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.9-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications Framework. CVSS 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).	4.7	More Details
CVE-2026-20060	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious web page.	4.7	More Details
CVE-2026-6652	A weakness has been identified in Pagekit CMS up to 1.0.18. This issue affects the function evaluate of the file app/modules/view/src/PhpEngine.php of the component StringStorage Template Handler. This manipulation causes improper neutralization of directives in dynamically evaluated code. 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.	4.7	More Details
CVE-2026-37346	SourceCodester Payroll Management and Information System v1.0 is vulnerable to SQL Injection in the file /payroll/view_account.php?emp_id=.	4.7	More Details
CVE-2026-40301	DOMSanitizer is a DOM/SVG/MathML Sanitizer for PHP 7.3+. Prior to version 1.0.10, DOMSanitizer::sanitize() allows <style> elements in SVG content but never inspects their text content. CSS url() references and @import rules pass through unfiltered, causing the browser to issue HTTP requests to attacker-controlled hosts when the sanitized SVG is rendered. Version 1.0.10 fixes the issue.	4.7	More Details
CVE-2026-6060	A vulnerability in the SQL Box in the admin interface of OTRS leads to an uncontrolled resource consumption leading to a DoS against the webserver. will be killed by the systemThis issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.3.X	4.5	More Details
CVE-2026-6058	** UNSUPPORTED WHEN ASSIGNED ** An improper encoding or escaping vulnerability in the CGI program of Zyxel WRE6505 v2 firmware version V1.00(ABDV.3)C0 could allow an adjacent attacker on the WLAN to cause a denial-of-service (DoS) condition in the web management interface by convincing an authenticated administrator to visit the “AP Select” page while a malformed SSID is present.	4.5	More Details
CVE-2026-3551	The Custom New User Notification plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's admin settings in all versions up to, and including, 1.2.0. This is due to insufficient input sanitization and output escaping on multiple settings fields including 'User Mail Subject', 'User From Name', 'User From Email', 'Admin Mail Subject', 'Admin From Name', and 'Admin From Email'. The settings are registered via register_setting() without sanitize callbacks, and the values retrieved via get_option() are echoed directly into HTML input value attributes without esc_attr(). This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in the plugin settings page that will execute whenever a user accesses that page. This could be used in multi-site installations where administrators of subsites could target super administrators.	4.4	More Details
CVE-2026-41330	OpenClaw before 2026.3.31 contains an environment variable override vulnerability in host exec policy that fails to properly enforce proxy, TLS, Docker, and Git TLS controls. Attackers can bypass security controls by overriding environment variables to circumvent proxy settings, TLS verification, Docker restrictions, and Git TLS enforcement.	4.4	More Details
CVE-2025-43935	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper resource shutdown or release vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.4	More Details
CVE-2026-2396	The List View Google Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the event description in all versions up to, and including, 7.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-6439	The VideoZen plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 1.0.1. This is due to insufficient input sanitization and output escaping in the videozen_conf() function. The 'lang' POST parameter is stored directly via update_option() without any sanitization, and later echoed inside a <textarea> element without applying esc_textarea() or any equivalent escaping function. This makes it possible for authenticated attackers with Administrator-level access and above to inject arbitrary web scripts into the plugin settings page that will execute whenever any user accesses that page.	4.4	More Details
	The OPEN-BRAIN plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'API Key' settings field in all versions		

CVE-2026-3995	up to, and including, 0.5.0. This is due to insufficient input sanitization and output escaping. The plugin uses sanitize_text_field() which strips HTML tags but does not encode double quotes or other HTML-special characters needed for safe attribute context output. The API key value is saved via update_option() and later output into an HTML input element's value attribute without esc_attr() escaping. This makes it possible for authenticated attackers, with Administrator-level access, to inject arbitrary web scripts via attribute breakout payloads (e.g., double quotes followed by event handlers) that execute whenever a user accesses the plugin settings page.	4.4	More Details
CVE-2026-6712	The Website LLMs.txt plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 8.2.6 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-2026-40590	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.214, the Change Customer modal exposes a “Create a new customer” flow via POST /customers/ajax with action=create. Under limited visibility, the endpoint drops unique-email validation. If the supplied email already belongs to a hidden customer, Customer::create() reuses that hidden customer object and fills empty profile fields from attacker-controlled input. Version 1.8.214 fixes the vulnerability.	4.3	More Details
CVE-2026-6797	A vulnerability was identified in Sanluan PublicCMS up to 6.202506.d. Affected by this vulnerability is the function ZipSecureFile.setMinflateRatio of the file common/src/main/java/com/publiccms/common/tools/DocToHtmlUtils.java. Such manipulation leads to resource consumption. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6796	A vulnerability was determined in Sanluan PublicCMS up to 6.202506.d. Affected is the function log_login of the file core/src/main/java/com/publiccms/controller/admin/LoginAdminController.java of the component Failed Login Handler. This manipulation of the argument errorPassword causes cleartext storage in a file or on disk. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-0971	An improper session timeout issue in Fortra's GoAnywhere MFT prior to version 7.10.0 results in SAML configured Web Users being redirected to the regular login page instead of the SAML login page.	4.3	More Details
CVE-2026-24176	NVIDIA KAI Scheduler contains a vulnerability where an attacker could cause improper authorization through cross-namespace pod references. A successful exploit of this vulnerability might lead to data tampering.	4.3	More Details
CVE-2026-34296	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Product Quality Management). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile Product Lifecycle Management for Process accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2026-41183	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.215, the assigned-only restriction is applied to direct conversation view and folder queries, but not to non-folder query builders. Global search and the AJAX filter path still reveal conversations that should be hidden. Version 1.8.215 fixes the vulnerability.	4.3	More Details
CVE-2026-22015	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2026-6564	A vulnerability was found in EMQ EMQX Enterprise up to 6.1.0. The impacted element is an unknown function of the component Session Handling. The manipulation results in improper authorization. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6598	A security vulnerability has been detected in langflow-ai langflow up to 1.8.3. The affected element is the function create_project/encrypt_auth_settings of the file src/backend/base/Langflow/api/v1/projects.py of the component Project Creation Endpoint. Such manipulation of the argument auth_settings leads to cleartext storage in a file or on disk. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-40486	Kimai is an open-source time tracking application. In versions 2.52.0 and below, the User Preferences API endpoint (PATCH /api/users/{id}/preferences) applies submitted preference values without checking the isEnabled() flag on preference objects. Although the hourly_rate and internal_rate fields are correctly marked as disabled for users lacking the hourly-rate role permission, the API ignores this restriction and saves the values directly. Any authenticated user can modify their own billing rates through this endpoint, resulting in unauthorized financial tampering affecting invoices and timesheet calculations. This issue has been fixed in version 2.53.0.	4.3	More Details
CVE-2026-40728	Missing Authorization vulnerability in BlockArt Magazine Blocks magazine-blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Magazine Blocks: from n/a through <= 1.8.3.	4.3	More Details
CVE-2026-40729	Missing Authorization vulnerability in bPlugins 3D viewer – Embed 3D Models 3d-viewer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects 3D viewer – Embed 3D Models: from n/a through <= 1.8.5.	4.3	More Details
CVE-	Missing Authorization vulnerability in Long Watch Studio MyRewards woorewards allows Exploiting Incorrectly Configured		More

2026-40786	Access Control Security Levels.This issue affects MyRewards: from n/a through <= 5.7.3.	4.3	Details
CVE-2025-53444	Cross-Site Request Forgery (CSRF) vulnerability in DeluxeThemes Userpro allows Cross Site Request Forgery.This issue affects Userpro: from n/a before 5.1.11.	4.3	More Details
CVE-2026-41285	In OpenBSD through 7.8, the slaacd and rad daemons have an infinite loop when they receive a crafted ICMPv6 Neighbor Discovery (ND) option (over a local network) with length zero, because of an "nd_opt_len * 8 - 2" expression with no preceding check for whether nd_opt_len is zero.	4.3	More Details
CVE-2026-20203	In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.6, 10.2.2510.10, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles, has write permission on the app, and does not hold the high-privilege capability `accelerate_datamodel`, could turn on or off Data Model Acceleration due to improper access control.	4.3	More Details
CVE-2025-15635	Cross-Site Request Forgery (CSRF) vulnerability in Zaytech Smart Online Order for Clover allows Cross Site Request Forgery.This issue affects Smart Online Order for Clover: from n/a through 1.6.0.	4.3	More Details
CVE-2026-20061	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to perform an SQL injection attack against an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP(S) request to the web-based management interface of an affected device. A successful exploit could allow the attacker to view data on the affected device.	4.3	More Details
CVE-2026-40305	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Starting in version 6.0.0 and prior to version 10.2.2, in the friends feature, a user could craft a request that would force the acceptance of a friend request on another user. Version 10.2.2 patches the issue.	4.3	More Details
CVE-2026-6441	The Canto plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 3.1.1. This is due to the absence of any capability check or nonce verification in the updateOptions() function, which is exposed via two AJAX hooks: wp_ajax_updateOptions (class-canto.php line 231) and wp_ajax_fbc_updateOptions (class-canto-settings.php line 76). Both hooks are registered exclusively under the wp_ajax_ prefix (requiring only a logged-in user), with no call to current_user_can() or check_ajax_referer(). This makes it possible for authenticated attackers with subscriber-level access and above to arbitrarily modify or delete plugin options controlling cron scheduling behavior (fbc_duplicates, fbc_cron, fbc_schedule, fbc_cron_time_day, fbc_cron_time_hour, fbc_cron_start) and to manipulate or clear the plugin's scheduled WordPress cron event (fbc_scheduled_update).	4.3	More Details
CVE-2026-6451	The cms-fuer-motorrad-werkstaetten plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.0.0. This is due to missing nonce validation on all eight AJAX deletion handlers: vehicles_cfmw_d_vehicle, contacts_cfmw_d_contact, suppliers_cfmw_d_supplier, receipts_cfmw_d_receipt, positions_cfmw_d_position, catalogs_cfmw_d_article, stock_cfmw_d_item, and settings_cfmw_d_catalog. None of these handlers call check_ajax_referer() or wp_verify_nonce(), nor do they perform any capability checks via current_user_can(). This makes it possible for unauthenticated attackers to delete arbitrary vehicles, contacts, suppliers, receipts, positions, catalog articles, stock items, or entire supplier catalogs via a forged request, provided they can trick a logged-in user into performing an action such as clicking a link to a malicious page.	4.3	More Details
CVE-2026-6591	A flaw has been found in ComfyUI up to 0.13.0. Affected is the function folder_paths.get_annotated_filepath of the file folder_paths.py of the component LoadImage Node. This manipulation of the argument Name causes path traversal. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-4002	The Petje.af plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to and including 2.1.8. This is due to missing nonce validation in the ajax_revoke_token() function which handles the 'petjeaf_disconnect' AJAX action. The function performs destructive operations including revoking OAuth2 tokens, deleting user meta, and deleting WordPress user accounts (for users with the 'petjeaf_member' role) without verifying the request originated from a legitimate source. This makes it possible for unauthenticated attackers to force authenticated users to delete their Petje.af member user accounts via a forged request granted the victim clicks on a link or visits a malicious site.	4.3	More Details
CVE-2023-5872	In Wago Smart Designer in versions up to 2.33.1 a low privileged remote attacker may enumerate projects and usernames through iterative requests to an specific endpoint.	4.3	More Details
CVE-2026-6293	The Inquiry Form to Posts or Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Stored Cross-Site Scripting in version 1.0. This is due to missing nonce validation on the plugin settings update handler, combined with insufficient input sanitization on all user-supplied fields and missing output escaping when rendering stored values. The settings handler fires solely on the presence of `$_POST['inq_hidden'] == 'Y'` with no call to `check_admin_referer()` and no WordPress nonce anywhere in the form or handler. This makes it possible for unauthenticated attackers to inject arbitrary web scripts via a forged request that tricks a logged-in Administrator into visiting a malicious page.	4.3	More Details
CVE-2026-4949	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 4.16.12. This is due to the 'process_checkout' function not properly enforcing the plan active status check when a 'change_plan_sub_id' parameter is provided. This makes it possible for authenticated attackers, with Subscriber-level access and above, to subscribe to inactive membership plans by supplying an arbitrary 'change_plan_sub_id' value in the checkout request.	4.3	More Details
CVE-2026-	The Responsive Blocks – Page Builder for Blocks & Patterns plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 2.2.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to modify global site-wide	4.3	More Details

6703	plugin configuration options, including toggling custom CSS, disabling blocks, changing layout defaults such as content width, container padding, and container gap, and altering auto-block-recovery behavior.		
CVE-2026-6559	A weakness has been identified in Wavlink WL-WN579A3 220323. This affects the function sub_401F80 of the file /cgi-bin/login.cgi. This manipulation of the argument Hostname causes cross site scripting. Remote exploitation of the attack is possible. Upgrading the affected component is recommended. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	4.3	More Details
CVE-2026-33214	Weblate is a web based localization tool. In versions prior to 5.17, the translation memory API exposed unintended endpoints, which in turn didn't enforce proper access control. This issue has been fixed in version 5.17. If users are unable to update immediately, they can work around this issue by blocking access to /api/memory/ in the HTTP server, which removes access to this feature.	4.3	More Details
CVE-2026-6590	A vulnerability was detected in ComfyUI up to 0.13.0. This impacts the function get_model_preview of the file app/model_manager.py of the component Model Preview Endpoint. The manipulation results in path traversal. The attack may be launched 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-2026-6589	A security vulnerability has been detected in ComfyUI up to 0.13.0. This affects the function create_origin_only_middleware of the file server.py. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-1541	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.15.1. This is due to the plugin's `fusion_get_post_custom_field()` function failing to validate whether metadata keys are protected (underscore-prefixed). This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract protected post metadata fields that should not be publicly accessible via the Dynamic Data feature's `post_custom_field` parameter.	4.3	More Details
CVE-2026-6601	A vulnerability has been found in Lagom WHMCS Template up to 2.4.2. This impacts an unknown function of the component Datatables. The manipulation leads to resource consumption. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-23777	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an exposure of sensitive information to an unauthorized actor vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	4.3	More Details
CVE-2026-6636	A vulnerability was detected in p2r3 convert up to 6998584ace3e11db66dff0b423612a5cf91de75b. Affected is the function Bun.serve of the file buildCache.js of the component API. Performing a manipulation of the argument pathname results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6487	A flaw has been found in Qihui jtbc5 CMS 5.0.3.6. Affected is an unknown function of the file /dev/code/common/diplomat/manage.php of the component Code Endpoint. This manipulation of the argument path causes path traversal. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-6298	Heap buffer overflow in Skia in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Critical)	4.3	More Details
CVE-2024-58343	Vision Helpdesk before 5.7.0 (patched in 5.6.10) allows attackers to read user profiles via modified serialized cookie data to vis_client_id.	4.3	More Details
CVE-2025-43883	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper check for unusual or exceptional conditions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.1	More Details
CVE-2026-39845	Weblate is a web based localization tool. In versions prior to 5.17, the webhook add-on did not utilize existing SSRF protections. This issue has been fixed in version 5.17. If developers are unable to update immediately, they can disable the webhook add-on as a workaround.	4.1	More Details
CVE-2026-40566	FreeScout is a free self-hosted help desk and shared mailbox. Versions prior to 1.8.213 have a Server-Side Request Forgery (SSRF) vulnerability in the IMAP/SMTP connection test functionality of FreeScout's `MailboxesController`. Three AJAX actions `fetch_test` (line 731), `send_test` (line 682), and `imap_folders` (line 773) in `app/Http/Controllers/MailboxesController.php` pass admin-configured `in_server`/`in_port` and `out_server`/`out_port` values directly to `fsockopen()` via `Helper::checkPort()` and to IMAP/SMTP client connections with zero SSRF protection. There is no IP validation, no hostname restriction, no blocklist of internal ranges, and no call to the project's own `sanitizeRemoteUrl()` or `checkUrlIpAndHost()` functions. The validation block in `connectionIncomingSave()` is entirely commented out. An authenticated admin can configure a mailbox's IMAP or SMTP server to point at any internal host and port, then trigger a connection test. The server opens raw TCP connections (via `fsockopen()`) and protocol-level connections (via IMAP client or SMTP transport) to the attacker-specified target. The response differentiates open from closed ports, enabling internal network port scanning. When the IMAP client connects to a non-IMAP service, the target's service banner or error response is captured in the IMAP debug log and returned in the AJAX response's `log` field, making this a semi-blind SSRF that enables service fingerprinting. In cloud environments, the metadata endpoint at `169[.]254[.]169[.]254` can be probed and partial response data may be leaked through protocol error messages. This is distinct from the `sanitizeRemoteUrl()` redirect bypass (freescout-3) -- different code	4.1	More Details

	path, different root cause, different protocol layer. Version 1.8.213 patches the vulnerability.		
CVE-2026-41282	ProjectDiscovery Nuclei 3 before 3.8.0 allows DSL expression injection. This affects use of -env-vars for multi-step templates against untrusted targets (not the default configuration).	4.0	More Details
CVE-2026-41254	Little CMS (lcms2) through 2.18 has an integer overflow in CubeSize in cmslut.c because the overflow check is performed after the multiplication.	4.0	More Details
CVE-2026-22014	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Workflow and Business Events). Supported versions that are affected are 12.2.7-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle User Management accessible data as well as unauthorized read access to a subset of Oracle User Management accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	3.8	More Details
CVE-2026-22008	Vulnerability in Oracle Java SE (component: Libraries). The supported version that is affected is Oracle Java SE: 25.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2026-6610	A vulnerability has been found in liangliangyy DjangoBlog up to 2.1.0.0. The impacted element is an unknown function of the file djangoblog/settings.py of the component Setting Handler. Such manipulation of the argument USER/PASSWORD leads to hard-coded credentials. The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is regarded as difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2026-40279	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.4.3, decode_signed32() in src/bacnet/bacint.c reconstructs a 32-bit signed integer from four APDU bytes using signed left shifts. When any of the four bytes has bit 7 set (value ≥ 0x80), the left-shift operation overflows a signed int32_t, which is undefined behavior per the C standard. This is flagged thousands of times per minute by UndefinedBehaviorSanitizer on any BACnet input containing signed-integer property values with high-bit-set bytes. This vulnerability is fixed in 1.4.3.	3.7	More Details
CVE-2026-32690	Secrets in Variables saved as JSON dictionaries were not properly redacted - in case thee variables were retrieved by the user the secrets stored as nested fields were not masked. If you do not store variables with sensitive values in JSON form, you are not affected. Otherwise please upgrade to Apache Airflow 3.2.0 that has the fix implemented	3.7	More Details
CVE-2025-31958	HCL BigFix Service Management is susceptible to HTTP Request Smuggling. HTTP request smuggling vulnerabilities arise when websites route HTTP requests through web servers with inconsistent HTTP parsing. HTTP Smuggling exploits inconsistencies in request parsing between front-end and back-end servers, allowing attackers to bypass security controls and perform attacks like cache poisoning or request hijacking.	3.7	More Details
CVE-2026-33877	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain a timing side-channel vulnerability in the password reset endpoint (/api/v1/@apostrophecms/login/reset-request) that allows unauthenticated username and email enumeration. When a user is not found, the handler returns after a fixed 2-second artificial delay, but when a valid user is found, it performs a MongoDB update and SMTP email send with no equivalent delay normalization, producing measurably different response times. The endpoint also accepts both username and email via an $or query, and has no rate limiting as the existing checkLoginAttempts throttle only applies to the login flow. This enables automated enumeration of valid accounts for use in credential stuffing or targeted phishing. Only instances that have explicitly enabled the passwordReset option are affected, as it defaults to false. This issue has been fixed in version 4.29.0.	3.7	More Details
CVE-2026-40263	Note Mark is an open-source note-taking application. In versions 0.19.1 and prior, the login endpoint performs bcrypt password verification only when the supplied username exists, returning immediately for nonexistent usernames. This timing discrepancy allows unauthenticated attackers to enumerate valid usernames by measuring response times, enabling targeted credential attacks. This issue has been fixed in version 0.19.2.	3.7	More Details
CVE-2026-22018	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2026-6493	A flaw has been found in lukevella rallly up to 4.7.4. This affects an unknown function of the file apps/web/src/app/[locale]/(auth)/reset-password/components/reset-password-form.tsx of the component Reset Password Handler. Executing a manipulation of the argument redirectTo can lead to cross site scripting. The attack can be executed remotely. The exploit has been published and may be used. Upgrading to version 4.8.0 mitigates this issue. Upgrading the affected component is advised. The vendor was contacted early about this disclosure.	3.5	More Details
CVE-	A vulnerability has been found in WebSystems WebTOTUM 2026. This impacts an unknown function of the component		

2026-6743	Calendar. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading the affected component is recommended. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	3.5	More Details
CVE-2024-7083	The Email Encoder WordPress plugin before 2.3.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	3.5	More Details
CVE-2026-6633	A security flaw has been discovered in Yifang CMS up to 2.0.5. The impacted element is the function store of the file plugins/yifang_backend_account/logic/admin/L_rbac_admin.php of the component Extended Management Module. The manipulation of the argument Account results in cross site scripting. The attack can be executed 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.	3.5	More Details
CVE-2026-6486	A vulnerability was detected in classroombookings up to 2.17.0. This impacts the function read of the file crbs-core/application/views/layout.php of the component User Display Name Handler. The manipulation of the argument displayname results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 2.17.1 will fix this issue. The patch is identified as 69c3c9bb8a17f1ea572d8f4502bf238f0214c98a. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	3.5	More Details
CVE-2026-6648	A vulnerability was found in Qibo CMS 1.0. Affected by this vulnerability is an unknown functionality of the component Internal Message Module. Performing a manipulation results in cross site scripting. 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.	3.5	More Details
CVE-2024-8010	The component accepts XML input through the publisher without disabling external entity resolution. This allows malicious actors to submit a crafted XML payload that exploits the unescaped external entity references. By leveraging this vulnerability, a malicious actor can read confidential files from the product's file system or access limited HTTP resources reachable via HTTP GET requests to the vulnerable product.	3.5	More Details
CVE-2026-6600	A flaw has been found in langflow-ai langflow up to 1.8.3. This affects an unknown function of the file src/frontend/src/modals/IOModal/components/chatView/chatMessage/components/edit-message.tsx of the component Frontend React Component Rendering. Executing a manipulation can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-6619	A vulnerability has been found in langgenius dify up to 1.13.3. Impacted is the function openInNewTab of the file web/app/components/base/image-uploader/image-preview.tsx of the component ImagePreview. The manipulation of the argument filename leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-40341	libgphoto2 is a camera access and control library. In versions up to and including 2.5.33, an out of bound read in ptp_unpack_EOS_FocusInfoEx could be used to crash libgphoto2 when processing input from untrusted USB devices. Commit c385b34af260595dfbb5f9329526be5158985987 contains a patch. No known workarounds are available.	3.5	More Details
CVE-2026-6745	A vulnerability was determined in Bagisto up to 2.3.15. Affected by this vulnerability is an unknown functionality of the component Custom Scripts Handler. This manipulation causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure and explains: "We already replied on the github advisories. All the security issues are addressed through security advisory. We will fix this in our upcomming releases."	3.5	More Details
CVE-2026-6592	A vulnerability has been found in ComfyUI up to 0.13.0. Affected by this vulnerability is the function getuserdata of the file app/user_manager.py of the component userdata Endpoint. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-6593	A vulnerability was found in ComfyUI up to 0.13.0. Affected by this issue is some unknown functionality of the file server.py of the component View Endpoint. Performing a manipulation results in cross site scripting. The attack is possible to be carried out 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.	3.5	More Details
CVE-2026-40334	libgphoto2 is a camera access and control library. In versions up to and including 2.5.33, a missing null terminator exists in ptp_unpack_Canon_FE() in camlibs/ptp2/ptp-pack.c (line 1377). The function copies a filename into a 13-byte buffer using strncpy without explicitly null-terminating the result. If the source data is exactly 13 bytes with no null terminator, the buffer is left unterminated, leading to out-of-bounds reads in any subsequent string operation. Commit 259fc7d3bfe534ce4b114c464f55b448670ab873 patches the issue.	3.5	More Details
CVE-2026-29179	October is a Content Management System (CMS) and web platform. Prior to 3.7.16 and 4.1.16, fine-grained sub-permission checks for asset and blueprint file operations were not enforced in the CMS and Tailor editor extensions. This only affects backend users who were explicitly granted editor access but had editor.cms_assets or editor.tailor_blueprints specifically withheld, an uncommon permission configuration. In this edge case, such users could perform file operations (create, delete, rename, move, upload) on theme assets or blueprint files despite lacking the required sub-permission. A related operator precedence error in the Tailor navigation also disclosed the theme blueprint directory tree under the same conditions. This vulnerability is fixed in 3.7.16 and 4.1.16.	3.3	More Details
CVE-2026-6830	nesquena hermes-webui contains an environment variable leakage vulnerability where profile switching does not clear environment variables from the previously active profile before loading the next profile. Attackers or users can exploit additive dotenv reload behavior to access provider API keys and other sensitive secrets from one profile context in another profile, breaking expected security isolation between profiles.	3.3	More Details

CVE-2026-21727	--- title: Cross-Tenant Legacy Correlation Disclosure and Deletion draft: false hero: image: /static/img/heros/hero-legal2.svg content: "# Cross-Tenant Legacy Correlation Disclosure and Deletion" date: 2026-01-29 product: Grafana severity: Low cve: CVE-2026-21727 cvss_score: "3.3" cvss_vector: "CVSS:3.3/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N" fixed_versions: - ">=11.6.11 >=12.0.9 >=12.1.6 >=12.2.4" --- A cross-tenant isolation vulnerability was found in Grafana's Correlations feature affecting legacy correlation records. Due to a backward compatibility condition allowing org_id = 0 records to be returned across organizations, a user with datasource management privileges could read and permanently delete legacy correlation data belonging to another organization. This issue affects correlations created prior to Grafana 10.2 and is fixed in >=11.6.11, >=12.0.9, >=12.1.6, and >=12.2.4. Thanks to Gyu-hyeok Lee (g2h) for reporting this vulnerability.	3.3	More Details
CVE-2026-40505	MuPDF before 1.27 contains an ANSI injection vulnerability in mutool that allows attackers to inject arbitrary ANSI escape sequences through crafted PDF metadata fields. Attackers can embed malicious ANSI escape codes in PDF metadata that are passed unsanitized to terminal output when running mutool info, enabling them to manipulate terminal display for social engineering attacks such as presenting fake prompts or spoofed commands.	3.3	More Details
CVE-2026-31369	PcManager is affected by type privilege bypass, successful exploitation of this vulnerability may affect service availability	3.2	More Details
CVE-2026-35249	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:N).	3.2	More Details
CVE-2026-39396	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.3, `ExtractPluginFromImage()` in OpenBao's OCI plugin downloader extracts a plugin binary from a container image by streaming decompressed tar data via `io.Copy` with no upper bound on the number of bytes written. An attacker who controls or compromises the OCI registry referenced in the victim's configuration can serve a crafted image containing a decompression bomb that decompresses to an arbitrarily large file. The SHA256 integrity check occurs after the full file is written to disk, meaning the hash mismatch is detected only after the damage (disk exhaustion) has already occurred. This allow the attacker to replace **legit plugin image** with no need to change its signature. Version 2.5.3 contains a patch.	3.1	More Details
CVE-2026-6611	A vulnerability was found in liangliangyy DjangoBlog up to 2.1.0.0. This affects an unknown function of the file djangoblog/settings.py of the component File Upload Endpoint. Performing a manipulation of the argument SECRET_KEY results in use of hard-coded cryptographic key . Remote exploitation of the attack is possible. The attack's complexity is rated as high. The exploitability is reported as difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-33436	Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. In versions prior to 2.0.0, file upload endpoints render user-supplied filenames directly into HTML using unsafe methods like innerHTML without sanitization. An attacker can craft a file with a malicious filename containing JavaScript that executes in the uploading user's browser context, resulting in reflected XSS. The issue affects numerous upload endpoints across the application. The issue has been fixed in version 2.0.0.	3.1	More Details
CVE-2026-3155	The OneSignal – Web Push Notifications plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 3.8.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete OneSignal metadata for arbitrary posts.	3.1	More Details
CVE-2026-33212	Weblate is a web based localization tool. In versions prior to 5.17, the tasks API didn't verify user access for pending tasks. This could expose logs of in-progress operations to users who don't have access to given scope. The attacker needs to brute-force the random UUID of the task, so exploiting this is unlikely with the default API rate limits. This issue has been fixed in version 5.17.	3.1	More Details
CVE-2026-6313	Insufficient policy enforcement in CORS in Google Chrome prior to 147.0.7727.101 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-2026-6312	Insufficient policy enforcement in Passwords in Google Chrome prior to 147.0.7727.101 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-2026-27937	October is a Content Management System (CMS) and web platform. Prior to 3.7.16 and 4.1.16, a reflected Cross-Site Scripting (XSS) vulnerability was identified in the backend DataTable widget where a query parameter was rendered without proper output escaping. This vulnerability is fixed in 3.7.16 and 4.1.16.	3.1	More Details
CVE-2026-40947	Yubico libfido2 before 1.17.0, python-fido2 before 2.2.0, and yubikey-manager before 5.9.1 have an unintended DLL search path.	2.9	More Details
CVE-2026-41080	libexpat before 2.7.6 uses insufficient entropy, and thus hash flooding can occur via a crafted XML document.	2.9	More Details
CVE-	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle		

2026-34268	GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 2.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2.9	More Details
CVE-2025-52641	HCL AION is affected by a vulnerability where certain system behaviours may allow exploration of internal filesystem structures. Exposure of such information may provide insights into the underlying environment, which could potentially aid in further targeted actions or limited information disclosure.	2.9	More Details
CVE-2026-22007	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 2.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2.9	More Details
CVE-2026-22001	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.0-8.0.45, 8.4.0-8.4.8 and 9.0.0-9.6.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.7	More Details
CVE-2026-6597	A weakness has been identified in langflow-ai langflow up to 1.8.3. Impacted is the function remove_api_keys/has_api_terms of the file src/backend/base/langflow/api/utils/core.py of the component Flow Using API. This manipulation causes unprotected storage of credentials. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2026-27769	Mattermost versions 10.11.x <= 10.11.12 fail to validate whether users were correctly owned by the correct Connected Workspace which allows a malicious remote server connected using the Conntexted Workspaces feature to change the displayed status of local users via the Connected Workspaces API.. Mattermost Advisory ID: MMSA-2026-00603	2.7	More Details
CVE-2026-6570	A security flaw has been discovered in kodcloud KodExplorer up to 4.52. Affected is the function initInstall of the file /app/controller/systemMember.class.php. Performing a manipulation of the argument path results in authorization bypass. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2026-6622	A vulnerability was identified in BichitroGan ISP Billing Software 2025.3.20. This affects an unknown function of the file /?_route=customers/edit/ of the component Customer Handler. Such manipulation leads to cross site scripting. 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.	2.4	More Details
CVE-2026-40336	libgphoto2 is a camera access and control library. Versions up to and including 2.5.33 have a memory leak in `ptp_unpack_Sony_DPD()` in `camlibs/ptp2/ptp-pack.c` (lines 884–885). When processing a secondary enumeration list (introduced in 2024+ Sony cameras), the function overwrites dpd->FORM.Enum.SupportedValue with a new calloc() without freeing the previous allocation from line 857. The original array and any string values it contains are leaked on every property descriptor parse. Commit 404ff02c75f3cb280196fc260a63c4d26cf1a8f6 fixes the issue.	2.4	More Details
CVE-2026-34312	Vulnerability in the RDBMS component of Oracle Database Server. Supported versions that are affected are 19.3-19.30. Easily exploitable vulnerability allows high privileged attacker having Row Access Method privilege with network access via multiple protocols to compromise RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.4	More Details
CVE-2026-6651	A security flaw has been discovered in erponline.xyz ERP Online up to 4.0.0. This vulnerability affects unknown code of the component Inventory Edit Item Page. The manipulation of the argument Item Name results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-6624	A weakness has been identified in BichitroGan ISP Billing Software 2025.3.20. Affected is an unknown function of the file /?_route=pool/add of the component Pool List Interface. Executing a manipulation can lead to cross site scripting. 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.	2.4	More Details
CVE-2026-6623	A security flaw has been discovered in BichitroGan ISP Billing Software 2025.3.20. This impacts an unknown function of the file /?_route=settings/users-view/ of the component Profile Page Handler. Performing a manipulation results in cross site scripting. The attack is possible to be carried out remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in	2.3	More

35250	unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 2.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).		Details
CVE-2025-15624	Plaintext Storage of a Password vulnerability in Sparx Systems Pty Ltd. Sparx Pro Cloud Server. In a setup where OpenID is used as the primary method of authentication to authenticate to Sparx EA, Pro Cloud Server creates local passwords to the users and stores them in plaintext.	N/A	More Details
CVE-2025-15623	Exposure of Private Personal Information to an Unauthorized Actor, : Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Sparx Systems Pty Ltd. Sparx Pro Cloud Server. Unauthenticated user can retrieve database password in plaintext in certain situations	N/A	More Details
CVE-2025-15622	Insufficiently Protected Credentials vulnerability in Sparx Systems Pty Ltd. Sparx Enterprise Architect. Client reveals plaintext OAuth2 client secretDesktop client decodes the secret and uses the plaintext secret to exchange it into an access and id tokens as part of the OpenID authentication flow.	N/A	More Details
CVE-2025-15625	Unauthenticated user is able to execute arbitrary SQL commands in Sparx Pro Cloud Server database in certain cases.	N/A	More Details
CVE-2026-5131	GREENmod uses named pipes for communication between plugins, the web portal, and the system service, but the access control lists for these pipes are configured incorrectly. This allows an attacker to communicate with the stream and upload any XML or JSON file, which will be processed by the named pipe with the privileges of the user under whose context the service is running. This allows for Server-Side Request Forgery to any Windows system on which the agent is installed and which provides communication via SMB or WebDav. This issue was fixed in version 2.8.33.	N/A	More Details
CVE-2026-27820	zlib is a Ruby interface for the zlib compression/decompression library. Versions 3.0.0 and below, 3.1.0, 3.1.1, 3.2.0 and 3.2.1 contain a buffer overflow vulnerability in the Zlib::GzipReader. The zstream_buffer_ungets function prepends caller-provided bytes ahead of previously produced output but fails to guarantee the backing Ruby string has enough capacity before the memmove shifts the existing data. This can lead to memory corruption when the buffer length exceeds capacity. This issue has been fixed in versions 3.0.1, 3.1.2 and 3.2.3.	N/A	More Details
CVE-2026-2336	A privilege escalation vulnerability in Microchip IStaX allows an authenticated low-privileged user to recover a shared per-device cookie secret from their own webstax_auth session cookie and forge a new cookie with administrative privileges.This issue affects IStaX before 2026.03.	N/A	More Details
CVE-2026-21719	An OS command injection vulnerability exists in CubeCart prior to 6.6.0, which may allow a user with an administrative privilege to execute an arbitrary OS command.	N/A	More Details
CVE-2026-6482	The Rapid7 Insight Agent (versions > 4.1.0.2) is vulnerable to a local privilege escalation attack that allows users to gain SYSTEM level control of a Windows host. Upon startup the agent service attempts to load an OpenSSL configuration file from a non-existent directory that is writable by standard users. By planting a crafted openssl.cnf file an attacker can trick the high-privilege service into executing arbitrary commands. This effectively permits an unprivileged user to bypass security controls and achieve a full host compromise under the agent’s SYSTEM level access.	N/A	More Details
CVE-2026-35496	A path traversal vulnerability exists in CubeCart prior to 6.6.0, which may allow a user with an administrative privilege to access higher-level directories that should not be accessible.	N/A	More Details
CVE-2023-20585	Insufficient checks of the RMP on host buffer access in IOMMU may allow an attacker with privileges and a compromised hypervisor to trigger an out of bounds condition without RMP checks, resulting in a potential loss of confidential guest integrity.	N/A	More Details
CVE-2026-40260	pypdf is a free and open-source pure-python PDF library. In versions prior to 6.10.0, manipulated XMP metadata entity declarations can exhaust RAM. An attacker who exploits this vulnerability can craft a PDF which leads to large memory usage. This requires parsing the XMP metadata. This issue has been fixed in version 6.10.0.	N/A	More Details
CVE-2026-40308	My Calendar is a WordPress plugin for managing calendar events. In versions 3.7.6 and below, the mc_ajax_mcjs_action AJAX endpoint, registered for unauthenticated users, passes user-supplied arguments through parse_str() without validation, allowing injection of arbitrary parameters including a site value. On WordPress Multisite installations, this enables an unauthenticated attacker to call switch_to_blog() with an arbitrary site ID and extract calendar events from any sub-site on the network, including private or hidden events. On standard Single Site installations, switch_to_blog() does not exist, causing an uncaught PHP fatal error and crashing the worker thread, creating an unauthenticated denial of service vector. This issue has been fixed in version 3.7.7.	N/A	More Details
CVE-2026-40248	free5GC is an open-source implementation of the 5G core network. In versions 4.2.1 and below of the UDR service, the handler for creating or updating Traffic Influence Subscriptions checks whether the influenceId path segment equals subs-to-notify, but does not return after sending the HTTP 404 response when validation fails. Execution continues and the subscription is created or overwritten regardless. An unauthenticated attacker with access to the 5G Service Based Interface can create or overwrite arbitrary Traffic Influence Subscriptions, including injecting attacker-controlled notificationUri values and arbitrary SUPIs, by supplying any value for the influenceId path segment. A patched version was not available at the time of publication.	N/A	More Details
CVE-2026-39313	mcp-framework is a framework for building Model Context Protocol (MCP) servers. In versions 0.2.21 and below, the readRequestBody() function in the HTTP transport concatenates request body chunks into a string with no size limit. Although a maxMessageSize configuration value exists, it is never enforced in readRequestBody(). A remote unauthenticated attacker can crash any mcp-framework HTTP server by sending a single large POST request to /mcp, causing memory exhaustion and denial of service. This issue has been fixed in version 0.2.22.	N/A	More Details
CVE-2025-	A missing lock verification in AMD Secure Processor (ASP) firmware may permit a locally authenticated attacker with administrative privileges to alter MMIO routing on some Zen 5-based products, potentially compromising guest system	N/A	More

54510	integrity.		Details
CVE-2025-54502	Incorrect use of boot service in the AMD Platform Configuration Blob (APCB) SMM driver could allow a privileged attacker with local access (Ring 0) to achieve privilege escalation potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2026-35469	spdystream is a Go library for multiplexing streams over SPDY connections. In versions 0.5.0 and below, the SPDY/3 frame parser does not validate attacker-controlled counts and lengths before allocating memory. Three allocation paths are affected: the SETTINGS frame entry count, the header count in parseHeaderValueBlock, and individual header field sizes — all read as 32-bit integers and used directly as allocation sizes with no bounds checking. Because SPDY header blocks are zlib-compressed, a small on-the-wire payload can decompress into large attacker-controlled values. A remote peer that can send SPDY frames to a service using spdystream can exhaust process memory and cause an out-of-memory crash with a single crafted control frame. This issue has been fixed in version 0.5.1.	N/A	More Details
CVE-2026-6762	Spoofing issue in the DOM: Core & HTML component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	N/A	More Details
CVE-2026-1564	Pega Platform versions 8.1.0 through 25.1.1 are affected by an HTML Injection vulnerability in a user interface component. Requires a high privileged user with a developer role.	N/A	More Details
CVE-2026-6409	A Denial of Service (DoS) vulnerability exists in the Protobuf PHP library during the parsing of untrusted input. Maliciously structured messages—specifically those containing negative varints or deep recursion—can be used to crash the application, impacting service availability.	N/A	More Details
CVE-2026-40943	Oxia is a metadata store and coordination system. Prior to 0.16.2, a race condition between session heartbeat processing and session closure can cause the server to panic with send on closed channel. The heartbeat() method uses a blocking channel send while holding a mutex, and under specific timing with concurrent close() calls, this can lead to either a deadlock (channel buffer full) or a panic (send on closed channel after TOCTOU gap in KeepAlive). This vulnerability is fixed in 0.16.2.	N/A	More Details
CVE-2026-40945	Oxia is a metadata store and coordination system. Prior to 0.16.2, when OIDC authentication fails, the full bearer token is logged at DEBUG level in plaintext. If debug logging is enabled in production, JWT tokens are exposed in application logs and any connected log aggregation system. This vulnerability is fixed in 0.16.2.	N/A	More Details
CVE-2026-40946	Oxia is a metadata store and coordination system. Prior to 0.16.2, the OIDC authentication provider unconditionally sets SkipClientIDCheck: true in the go-oidc verifier configuration, disabling the standard audience (aud) claim validation at the library level. This allows tokens issued for unrelated services by the same OIDC issuer to be accepted by Oxia. This vulnerability is fixed in 0.16.2.	N/A	More Details
CVE-2026-5598	Covert timing channel vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA core on all (core modules). This vulnerability is associated with program files FrodoEngine.Java. This issue affects BC-JAVA: from 1.71 before 1.84.	N/A	More Details
CVE-2026-5588	Use of a Broken or Risky Cryptographic Algorithm vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcpkix on all (pkix modules), Legion of the Bouncy Castle Inc. BCPKIX-FIPS bcpkix on All (pkix modules). This vulnerability is associated with program files JcaContentVerifierProviderBuilder.Java. This issue affects BC-JAVA: from 1.67 before 1.84; BCPKIX-FIPS: from 2.0.6 before 2.0.11, from 2.1.7 before 2.1.11.	N/A	More Details
CVE-2026-3505	Allocation of resources without limits or throttling, Uncontrolled Resource Consumption vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcpg on all (pg modules). This vulnerability is associated with program files AEADEncDataPacket.Java, BcAEADUtil.Java, JceAEADUtil.Java, OperatorHelper.Java. This issue affects BC-JAVA: from 1.74 before 1.84.	N/A	More Details
CVE-2026-3307	An authorization bypass vulnerability was identified in GitHub Enterprise Server that allowed an attacker with admin access on one repository to modify the secret scanning push protection delegated bypass reviewer list on another repository by manipulating the owner_id parameter in the request body. Authorization was verified against the repository in the URL, but the action was applied to a different repository specified in the request body. The impact is limited to assigning existing trusted users as bypass reviewers; it does not allow adding arbitrary external users. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.14.25, 3.15.20, 3.16.16, 3.17.13, 3.18.7, 3.19.4 and 3.20.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-33808	Impact@fastify/express v4.0.4 and earlier fails to normalize URLs before passing them to Express middleware when Fastify router normalization options are enabled. This allows complete bypass of path-scoped authentication middleware via duplicate slashes when ignoreDuplicateSlashes is enabled, or via semicolon delimiters when useSemicolonDelimiter is enabled. In both cases, Fastify router normalizes the URL and matches the route, but @fastify/express passes the original un-normalized URL to Express middleware, which fails to match and is skipped. An unauthenticated attacker can access protected routes by manipulating the URL path. PatchesUpgrade to @fastify/express v4.0.5 or later.	N/A	More Details
CVE-2026-0636	Improper neutralization of special elements used in an LDAP query ('LDAP injection') vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcprov on all (prov modules). This vulnerability is associated with program files LDAPStoreHelper. This issue affects BC-JAVA: from 1.74 before 1.84.	N/A	More Details
CVE-2025-14813	Use of a Broken or Risky Cryptographic Algorithm vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcprov on all (core modules). This vulnerability is associated with program files G3413CTRBlockCipher. GOSTCTR implementation unable to process more than 255 blocks correctly. This issue affects BC-JAVA: from 1.59 before 1.84.	N/A	More Details
CVE-2026-26291	Stored cross-site scripting vulnerability exists in GROWI v7.4.6 and earlier. If this vulnerability is exploited, an arbitrary script may be executed in a user's web browser.	N/A	More Details

CVE-2026-6328	Improper input validation, Improper verification of cryptographic signature vulnerability in XQUIC Project XQUIC xquic on Linux (QUIC protocol implementation, packet processing module, STREAM frame handler modules) allows Protocol Manipulation.This issue affects XQUIC: through 1.8.3.	N/A	More Details
CVE-2026-40499	radare2 prior to version 6.1.4 contains a command injection vulnerability in the PDB parser's print_gvars() function that allows attackers to execute arbitrary commands by embedding a newline byte in the PE section header name field. Attackers can craft a malicious PDB file with specially crafted section names to inject r2 commands that are executed when the idp command processes the file.	N/A	More Details
CVE-2026-40105	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Versions 10.4-rc-1, through 16.10.15, 17.0.0-rc-1, through 17.4.7 and 17.5.0-rc-1 through 17.10.0 contain a reflected cross-site scripting vulnerability (XSS) in the comparison view between revisions of a page allows executing JavaScript code in the user's browser. If the current user is an admin, this can not only affect the current user but also the confidentiality, integrity and availability of the whole XWiki instance. If developers are unable to update immediately, they can apply the patch manually to templates/changesdoc.vm in the deployed WAR.	N/A	More Details
CVE-2026-40096	immich is a high performance self-hosted photo and video management solution. Versions prior to 2.7.3 contain an open redirect vulnerability in the shared album functionality, where the album name is inserted unsanitized into a <meta> tag in api.service.ts. A registered attacker can create a shared album with a crafted name containing 0;url=https://attackersite.com" http-equiv="refresh, which when rendered in the <meta property="og:title"> tag causes the victim's browser to redirect to an attacker-controlled site upon opening the share link. This facilitates phishing attacks, as the attacker could host a modified version of immich that collects login credentials from victims who believe they need to authenticate to view the shared album. This issue has been fixed in version 2.7.3.	N/A	More Details
CVE-2026-4296	An incorrect regular expression vulnerability was identified in GitHub Enterprise Server that allowed an attacker to bypass OAuth redirect URI validation. An attacker with knowledge of a first-party OAuth application's registered callback URL could craft a malicious authorization link that, when clicked by a victim, would redirect the OAuth authorization code to an attacker-controlled domain. This could allow the attacker to gain unauthorized access to the victim's account with the scopes granted to the OAuth application. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.20.1, 3.19.5, 3.18.8, 3.17.14, 3.16.17, 3.15.21, 3.14.26. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-4821	An improper neutralization of special elements vulnerability was identified in GitHub Enterprise Server that allowed an authenticated Management Console administrator to execute arbitrary OS commands via shell metacharacter injection in proxy configuration fields such as http_proxy. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and administrator privileges to the Management Console. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.20.1, 3.19.5, 3.18.8, 3.17.14, 3.16.17, 3.15.21, 3.14.26. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-4872	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-5512	An improper authorization vulnerability was identified in GitHub Enterprise Server that allowed an authenticated attacker to determine the names of private repositories by their numeric ID. The mobile upload policy API endpoint did not perform an early authorization check, and validation error messages included the full repository name for repositories the caller did not have access to. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.20.1, 3.19.5, 3.18.8, 3.17.14, 3.16.17, 3.15.21, and 3.14.26. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-5845	An improper authorization vulnerability in scoped user-to-server (ghu_) token authorization in GitHub Enterprise Server allows an authenticated attacker to access private repositories outside the intended installation scope, which can include write operations, via an authorization fallback that treated a revoked/deleted installation as a global installation context, which could be chained with token revocation timing and SSH push attribution to obtain and reuse a victim-scoped token. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.20.1, 3.19.5, 3.18.8, 3.17.14, 3.16.17, 3.15.21, and 3.14.26. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-40944	Oxia is a metadata store and coordination system. Prior to 0.16.2, the trustedCertPool() function in the TLS configuration only parses the first PEM block from CA certificate files. When a CA bundle contains multiple certificates (e.g., intermediate + root CA), only the first certificate is loaded. This silently breaks certificate chain validation for mTLS. This vulnerability is fixed in 0.16.2.	N/A	More Details
CVE-2026-40942	The Data Sharing Framework (DSF) implements a distributed process engine based on the BPMN 2.0 and FHIR R4 standards. Prior to 2.1.0, The OIDC JWKS and Metadata Document caches used an inverted time comparison (isBefore instead of isAfter), causing the cache to never return cached values. Every incoming request triggered a fresh HTTP fetch of the OIDC Metadata Document and JWKS keys from the OIDC provider. The OIDC token cache for the FHIR client connections used an inverted time comparison (isBefore instead of isAfter), causing the cache to never invalidate. Every incoming request returned the same OIDC token even if expired. This vulnerability is fixed in 2.1.0.	N/A	More Details
CVE-2026-5968	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-40939	The Data Sharing Framework (DSF) implements a distributed process engine based on the BPMN 2.0 and FHIR R4 standards. Prior to 2.1.0, OIDC-authenticated sessions had no configured maximum inactivity timeout. Sessions persisted indefinitely after login, even after the OIDC access token expired. This vulnerability is fixed in 2.1.0.	N/A	More Details
CVE-2025-15621	Insufficiently Protected Credentials in Sparx Systems Pty Ltd. Sparx Enterprise Architect. Client does not verify the receiver of OAuth2 credentials during OpenID authentication	N/A	More Details

CVE-2026-40118	UDP Console provided by Arcserve contains an incorrectly specified destination in a communication channel vulnerability. When a user configures an activation server hostname of the affected product to a dummy URL, the product may unintentionally communicate with the dummy domain, causing information disclosure.	N/A	More Details
CVE-2026-6349	The iSherlock developed by HGiga has an OS Command Injection vulnerability, allowing unauthenticated local attackers to inject arbitrary OS commands and execute them on the server.	N/A	More Details
CVE-2026-3428	A Download of Code Without Integrity Check vulnerability in the update modules in ASUS Member Center(华硕大厅) allows a local user to achieve privilege escalation to Administrator via exploitation of a Time-of-check Time-of-use (TOC-TOU) during the update process, where an unexpected payload is substituted for a legitimate one immediately after download, and subsequently executed with administrative privileges upon user consent. Refer to the 'Security Update for ASUS Member Center' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-1880	An Incorrect Permission Assignment for Critical Resource vulnerability in the ASUS DriverHub update process allows privilege escalation due to improper protection of required execution resources during the validation phase, permitting a local user to make unprivileged modifications. This allows the altered resource to pass system checks and be executed with elevated privileges upon a user-initiated update. Refer to the 'Security Update for ASUS DriverHub' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-5363	Inadequate Encryption Strength vulnerability in TP-Link Archer C7 v5 and v5.8 (uhttpd modules) allows Password Recovery Exploitation. The web interface encrypts the admin password client-side using RSA-1024 before sending it to the router during login. An adjacent attacker with the ability to intercept network traffic could potentially perform a brute-force or factorization attack against the 1024-bit RSA key to recover the plaintext administrator password, leading to unauthorized access and compromise of the device configuration. This issue affects Archer C7: through Build 20220715.	N/A	More Details
CVE-2026-40192	Pillow is a Python imaging library. Versions 10.3.0 through 12.1.1 did not limit the amount of GZIP-compressed data read when decoding a FITS image, making them vulnerable to decompression bomb attacks. A specially crafted FITS file could cause unbounded memory consumption, leading to denial of service (OOM crash or severe performance degradation). If users are unable to immediately upgrade, they should only open specific image formats, excluding FITS, as a workaround.	N/A	More Details
CVE-2026-40179	Prometheus is an open-source monitoring system and time series database. Versions 3.0 through 3.5.1 and 3.6.0 through 3.11.1 have stored cross-site scripting vulnerabilities in multiple components of the Prometheus web UI where metric names and label values are injected into innerHTML without escaping. In both the Mantine UI and old React UI, chart tooltips on the Graph page render metric names containing HTML/JavaScript without sanitization. In the old React UI, the Metric Explorer fuzzy search results use dangerouslySetInnerHTML without escaping, and heatmap cell tooltips interpolate le label values without sanitization. With Prometheus v3.x defaulting to UTF-8 metric and label name validation, characters like <, >, and " are now valid in metric names and labels. An attacker who can inject metrics via a compromised scrape target, remote write, or OTLP receiver endpoint can execute arbitrary JavaScript in the browser of any Prometheus user who views the metric in the Graph UI, potentially enabling configuration exfiltration, data deletion, or Prometheus shutdown depending on enabled flags. This issue has been fixed in versions 3.5.2 and 3.11.2. If developers are unable to immediately update, the following workarounds are recommended: ensure that the remote write receiver (--web.enable-remote-write-receiver) and the OTLP receiver (--web.enable-otlp-receiver) are not exposed to untrusted sources; verify that all scrape targets are trusted and not under attacker control; avoid enabling admin or mutating API endpoints (e.g., --web.enable-admin-api or --web.enable-lifecycle) in environments where untrusted data may be ingested; and refrain from clicking untrusted links, particularly those containing functions such as label_replace, as they may generate poisoned label names and values.	N/A	More Details
CVE-2026-1711	Pega Platform versions 8.1.0 through 25.1.1 are affected by a Stored Cross-Site Scripting vulnerability in a user interface component. Requires a high privileged user with a developer role.	N/A	More Details
CVE-2026-40320	Giskard is an open-source testing framework for AI models. In versions prior to 1.0.2b1, the ConformityCheck class rendered the rule parameter through Jinja2's default Template() constructor, silently interpreting template expressions at runtime. If check definitions are loaded from an untrusted source, a crafted rule string could achieve arbitrary code execution. Exploitation requires write access to a check definition and subsequent execution of the test suite. This issue has been fixed in giskard-checks version 1.0.2b1.	N/A	More Details
CVE-2026-6398	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-5189	CWE-798: Use of Hard-coded Credentials in Sonatype Nexus Repository Manager versions 3.0.0 through 3.70.5 allows an unauthenticated attacker with network access to gain unauthorized read/write access to the internal database and execute arbitrary OS commands as the Nexus process user. Exploitation requires the non-default nexus.orient.binaryListenerEnabled=true configuration to be enabled.	N/A	More Details
CVE-2026-40892	PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, a stack buffer overflow exists in pjsip_auth_create_digest2() in PJSIP when using pre-computed digest credentials (PJSIP_CRED_DATA_DIGEST). The function copies credential data using cred_info->data.slen as the length without an upper-bound check, which can overflow the fixed-size ha1 stack buffer (128 bytes) if data.slen exceeds the expected digest string length.	N/A	More Details
CVE-2026-40895	follow-redirects is an open source, drop-in replacement for Node's `http` and `https` modules that automatically follows redirects. Prior to 1.16.0, when an HTTP request follows a cross-domain redirect (301/302/307/308), follow-redirects only strips authorization, proxy-authorization, and cookie headers (matched by regex at index.js). Any custom authentication header (e.g., X-API-Key, X-Auth-Token, Api-Key, Token) is forwarded verbatim to the redirect target. This vulnerability is fixed in 1.16.0.	N/A	More Details
CVE-2025-15610	Deserialization of untrusted data vulnerability in OpenText, Inc RightFax on Windows, 64 bit, 32 bit allows Object Injection.This issue affects RightFax: through 25.4.	N/A	More Details

CVE-2026-5387	The vulnerability, if exploited, could allow an unauthenticated miscreant to perform operations intended only for Simulator Instructor or Simulator Developer (Administrator) roles, resulting in privilege escalation with potential for modification of simulation parameters, training configuration, and training records.	N/A	More Details
CVE-2026-4682	Certain HP DeskJet All in One devices may be vulnerable to remote code execution caused by a buffer overflow when specially crafted Web Services for Devices (WSD) scan requests are improperly validated and handled by the MFP. WSD Scan is a Microsoft Windows–based network scanning protocol that allows a PC to discover scanners (and MFPs) on a network and send scan jobs to them without requiring vendor specific drivers or utilities.	N/A	More Details
CVE-2026-4667	HP System Optimizer might potentially be vulnerable to escalation of privilege. HP is releasing an update to mitigate this potential vulnerability.	N/A	More Details
CVE-2026-33805	@fastify/reply-from v12.6.1 and earlier and @fastify/http-proxy v11.4.3 and earlier process the client's Connection header after the proxy has added its own headers via rewriteRequestHeaders. This allows attackers to retroactively strip proxy-added headers from upstream requests by listing them in the Connection header value. Any header added by the proxy for routing, access control, or security purposes can be selectively removed by a client. @fastify/http-proxy is also affected as it delegates to @fastify/reply-from. Upgrade to @fastify/reply-from v12.6.2 or @fastify/http-proxy v11.4.4 or later.	N/A	More Details
CVE-2026-40319	Giskard is an open-source testing framework for AI models. In versions prior to 1.0.2b1, the RegexMatching check passes a user-supplied regular expression pattern directly to Python's re.search() without any timeout or complexity guard. A crafted regex pattern can trigger catastrophic backtracking, causing the process to hang indefinitely. Exploitation requires write access to a check definition and subsequent execution of the test suite. This issue has been fixed in giskard-checks version 1.0.2b1.	N/A	More Details
CVE-2026-5250	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-28214	Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, the ClumpletReader::getClumpletSize() function can overflow the totalLength value when parsing a Wide type clumplet, causing an infinite loop. An authenticated user with INSERT privileges on any table can exploit this via a crafted Batch Parameter Block to cause a denial of service against the server. This issue has been fixed in versions 5.0.4, 4.0.7 and 3.0.14.	N/A	More Details
CVE-2026-31430	In the Linux kernel, the following vulnerability has been resolved: X.509: Fix out-of-bounds access when parsing extensions Leo reports an out-of-bounds access when parsing a certificate with empty Basic Constraints or Key Usage extension because the first byte of the extension is read before checking its length. Fix it. The bug can be triggered by an unprivileged user by submitting a specially crafted certificate to the kernel through the keyrings(7) API. Leo has demonstrated this with a proof-of-concept program responsibly disclosed off-list.	N/A	More Details
CVE-2025-41029	SQL injection vulnerability in Zeon Academy Pro by Zeon Global Tech. This vulnerability allows an attacker to retrieve, create, update, and delete databases by sending a POST request using the parameter 'phonenumber' in '/private/continue-upload.php'.	N/A	More Details
CVE-2026-22051	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9.0.13 and 12.0.0.6 are susceptible to a Information Disclosure vulnerability. Successful exploit could allow an authenticated attacker with low privileges to run arbitrary metrics queries, revealing metric results that they do not have access to.	N/A	More Details
CVE-2026-40498	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, an unauthenticated attacker can access diagnostic and system tools that should be restricted to administrators. The /system/cron endpoint relies on a static MD5 hash derived from the APP_KEY, which is exposed in the response and logs. Accessing these endpoints reveals sensitive server information (Full Path Disclosure), process IDs, and allows for Resource Exhaustion (DoS) by triggering heavy background tasks repeatedly without any rate limiting. The cron hash is generated using md5(APP_KEY . 'web_cron_hash'). Since this hash is often transmitted via GET requests, it is susceptible to exposure in server logs, browser history, and proxy logs. Furthermore, the lack of rate limiting on these endpoints allows for automated resource exhaustion (DoS) and brute-force attempts. Version 1.8.213 fixes the issue.	N/A	More Details
CVE-2026-0930	Potential read out of bounds case with wolfSSHd on Windows while handling a terminal resize request. An authenticated user could trigger the out of bounds read after establishing a connection which would leak the adjacent stack memory to the pseudo-console output.	N/A	More Details
CVE-2019-25714	Seeyon OA A8 contains an unauthenticated arbitrary file write vulnerability in the /seeyon/htmlofficeservlet endpoint that allows remote attackers to write arbitrary files to the web application root by sending specially crafted POST requests with custom base64-encoded payloads. Attackers can write JSP webshells to the web root and execute them through the web server to achieve arbitrary OS command execution with web server privileges. Exploitation evidence was first observed by the Shadowserver Foundation on 2021-03-26 (UTC).	N/A	More Details
CVE-2026-21571	This Critical severity OS Command Injection vulnerability was introduced in versions 9.6.0, 10.0.0, 10.1.0, 10.2.0, 11.0.0, 11.1.0, 12.0.0, and 12.1.0 of Bamboo Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 9.4 and a CVSS Vector of CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H allows an authenticated attacker to execute commands on the remote system, which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Bamboo Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bamboo Data Center 9.6.0: Upgrade to a release greater than or equal to 9.6.25 Bamboo Data Center 10.2: Upgrade to a release greater than or equal to 10.2.18 Bamboo Data Center 12.1: Upgrade to a release greater than or equal to 12.1.6 See the release notes ([https://confluence.atlassian.com/bamboorelease s/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center from the download center ([https://www.atlassian.com/software/bamboo/download-archives]).	N/A	More Details
CVE-	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.5, all WebSocket endpoints in nginx-ui use a gorilla/websocket Upgrader with CheckOrigin unconditionally returning true, allowing Cross-Site WebSocket Hijacking		

2026-34403	(CSWSH). Combined with the fact that authentication tokens are stored in browser cookies (set via JavaScript without HttpOnly or explicit SameSite attributes), a malicious webpage can establish authenticated WebSocket connections to the nginx-ui instance when a logged-in administrator visits the attacker-controlled page. Version 2.3.5 patches the issue.	N/A	More Details
CVE-2026-33432	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions up to and including 8.2.8.2, when LDAP authentication is enabled, Roxy-WI constructs an LDAP search filter by directly concatenating the user-supplied login username into the filter string without escaping LDAP special characters. An unauthenticated attacker can inject LDAP filter metacharacters into the username field to manipulate the search query, cause the directory to return an unintended user entry, and bypass authentication entirely — gaining access to the application without knowing any valid password. As of time of publication, no known patches are available.	N/A	More Details
CVE-2026-33431	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.4, the POST /config/<service>/show API endpoint accepts a configver parameter that is directly appended to a base directory path to construct a local file path, which is subsequently opened and its contents returned to the caller. The existing path traversal guard only inspects the base directory variable (which is never user-controlled) and entirely ignores the user-supplied configver value. An authenticated attacker can supply a configver value containing `../` sequences to escape the intended directory and read arbitrary files accessible to the web application process. Version 8.2.6.4 contains a patch for the issue.	N/A	More Details
CVE-2026-33031	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, a user who was disabled by an administrator can use previously issued API tokens for up to the token lifetime. In practice, disabling a compromised account does not actually terminate that user’s access, so an attacker who already stole a JWT can continue reading and modifying protected resources after the account is marked disabled. Since tokens can be used to create new accounts, it is possible the disabled user to maintain the privilege. Version 2.3.4 patches the issue.	N/A	More Details
CVE-2026-32311	Flowsint is an open-source OSINT graph exploration tool designed for cybersecurity investigation, transparency, and verification. 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. The nodes can have automated processes execute on them called 'transformers'. A remote attacker can create a sketch, then trigger the 'org_to_asn' transform on an organization node to execute arbitrary OS commands as root on the host machine via shell metacharacters and a docker container escape. Commit b52cbbb904c8013b74308d58af88bc7dbb1b055c appears to remove the code that causes this issue.	N/A	More Details
CVE-2026-32135	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Versions prior to 0.24.11 have a remotely triggerable heap buffer overflow in the `uri_param_parse` function of NanoMQ's REST API. The vulnerability occurs due to an off-by-one error when allocating memory for query parameter keys and values, allowing an attacker to write a null byte beyond the allocated buffer. This can be triggered via a crafted HTTP request. Version 0.24.11 patches the issue.	N/A	More Details
CVE-2026-30452	Textpattern CMS 4.9.0 contains a Broken Access Control vulnerability in the article management system that allows authenticated users with low privileges to modify articles owned by users with higher privileges. By manipulating the article ID parameter during the duplicate-and-save workflow in textpattern/include/txp_article.php, an attacker can bypass authorization checks and overwrite content belonging to other users.	N/A	More Details
CVE-2025-11249	Rejected reason: This CVE id was assigned as a duplicate of CVE-2025-66414.	N/A	More Details
CVE-2026-23758	GFI HelpDesk before 4.99.9 contains a stored cross-site scripting vulnerability in the ticket subject field that allows authenticated staff members to inject malicious JavaScript by manipulating the editsubject POST parameter. Attackers can inject XSS payloads through inadequate sanitization in Controller_Ticket.EditSubmit() that bypass the incomplete SanitizeForXSS() method to execute arbitrary JavaScript when other staff members or administrators view the affected ticket.	N/A	More Details
CVE-2026-38835	Tenda W30E V2.0 V16.01.0.21 was found to contain a command injection vulnerability in the formSetUSBPartitionUmount function via the usbPartitionName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	N/A	More Details
CVE-2026-40488	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 version 20.17.0, the product custom option file upload in OpenMage LTS uses an incomplete blocklist (`forbidden_extensions = php,exe`) to prevent dangerous file uploads. This blocklist can be trivially bypassed by using alternative PHP-executable extensions such as `.phtml`, `.phar`, `.php3`, `.php4`, `.php5`, `.php7`, and `.pht`. Files are stored in the publicly accessible `media/custom_options/quote/` directory, which lacks server-side execution restrictions for some configurations, enabling Remote Code Execution if this directory is not explicitly denied script execution. Version 20.17.0 patches the issue.	N/A	More Details
CVE-2026-40098	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 version 20.17.0, the shared wishlist add-to-cart endpoint authorizes access with a public `sharing_code`, but loads the acted-on wishlist item by a separate global `wishlist_item_id` and never verifies that the item belongs to the shared wishlist referenced by that code. This lets an attacker use a valid shared wishlist code for wishlist A and a wishlist item ID belonging to victim wishlist B to import victim item B into the attacker's cart through the shared wishlist flow for wishlist A. Because the victim item's stored `buyRequest` is reused during cart import, the victim's private custom-option data is copied into the attacker's quote. If the product uses a file custom option, this can be elevated to cross-user file disclosure because the imported file metadata is preserved and the download endpoint is not ownership-bound. Version 20.17.0 patches the issue.	N/A	More Details
CVE-2026-40570	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, the `load_customer_info` action in `POST /conversation/ajax` returns complete customer profile data to any authenticated user without verifying mailbox access. An attacker only needs a valid email address to retrieve all customer PII. Version 1.8.213 fixes the issue.	N/A	More Details
CVE-2026-3219	pip handles concatenated tar and ZIP files as ZIP files regardless of filename or whether a file is both a tar and ZIP file. This behavior could result in confusing installation behavior, such as installing "incorrect" files according to the filename of the archive. New behavior only proceeds with installation if the file identifies uniquely as a ZIP or tar archive, not as both.	N/A	More Details

CVE-2026-40583	UltraDAG is a minimal DAG-BFT blockchain in Rust. In version 0.1, a non-council attacker can submit a signed SmartOp::Vote transaction that passes signature, nonce, and balance prechecks, but fails authorization only after state mutation has already occurred.	N/A	More Details
CVE-2026-40584	RansomLook is a tool to monitor Ransomware groups and markets and extract their victims. Prior to 1.9.0, the API in the affected application improperly filters private location entries in website/web/api/genericapi.py. Because the code removes elements from a list while iterating over it, entries marked as private may be unintentionally retained in API responses, allowing unauthorized disclosure of non-public location information. This vulnerability is fixed in 1.9.0.	N/A	More Details
CVE-2026-6369	An improper access control vulnerability in the canonical-livepatch snap client prior to version 10.15.0 allows a local unprivileged user to obtain a sensitive, root-level authentication token by sending an unauthenticated request to the livepatchd.sock Unix domain socket. This vulnerability is exploitable on systems where an administrator has already enabled the Livepatch client with a valid Ubuntu Pro subscription. This token allows an attacker to access Livepatch services using the victim's credentials, as well as potentially cause issues to the Livepatch server.	N/A	More Details
CVE-2025-41011	HTML injection vulnerability in PHP Point of Sale v19.4. This vulnerability allows an attacker to render HTML in the victim's browser due to a lack of proper validation of user input by sending a request to '/reports/generate/specific_customer', ussing 'start_date_formatted' y 'end_date_formatted' parameters.	N/A	More Details
CVE-2026-5789	Vulnerability related to an unquoted search path in CivetWeb v1.16. This vulnerability allows a local attacker to execute arbitrary code with elevated privileges by placing a malicious executable in a directory that is scanned before the intended application path (C:\Program Files\CivetWeb\CivetWeb.exe --), due to the absence of quotes in the service configuration.	N/A	More Details
CVE-2026-3298	The method "sock_recvfrom_into()" of "asyncio.ProacterEventLoop" (Windows only) was missing a boundary check for the data buffer when using nbytes parameter. This allowed for an out-of-bounds buffer write if data was larger than the buffer size. Non-Windows platforms are not affected.	N/A	More Details
CVE-2025-13826	Zervit's portable HTTP/web server is vulnerable to remote DoS attacks when a configuration reset request is made. The vulnerability is caused by inadequate validation of user-supplied input. An attacker can exploit this vulnerability by sending malicious requests. If the vulnerability is successfully exploited, the application can be made to stop responding, resulting in a DoS condition. It is possible to manually restart the application.	N/A	More Details
CVE-2026-6757	Invalid pointer in the JavaScript: WebAssembly component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	N/A	More Details
CVE-2026-6756	Mitigation bypass in Firefox for Android. This vulnerability was fixed in Firefox 150.	N/A	More Details
CVE-2026-6753	Incorrect boundary conditions in the WebRTC component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	N/A	More Details
CVE-2026-32147	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP ssh (ssh_sftpd module) allows an authenticated SFTP user to modify file attributes outside the configured chroot directory. The SFTP daemon (ssh_sftpd) stores the raw, user-supplied path in file handles instead of the chroot-resolved path. When SSH_FXP_FSETSTAT is issued on such a handle, file attributes (permissions, ownership, timestamps) are modified on the real filesystem path, bypassing the root directory boundary entirely. Any authenticated SFTP user on a server configured with the root option can modify file attributes of files outside the intended chroot boundary. The prerequisite is that a target file must exist on the real filesystem at the same relative path. Note that this vulnerability only allows modification of file attributes; file contents cannot be read or altered through this attack vector. If the SSH daemon runs as root, this enables direct privilege escalation: an attacker can set the setuid bit on any binary, change ownership of sensitive files, or make system configuration world-writable. This vulnerability is associated with program files lib/ssh/src/ssh_sftpd.erl and program routines ssh_sftpd:do_open/4 and ssh_sftpd:handle_op/4. This issue affects OTP from OTP 17.0 until OTP 28.4.3, 27.3.4.11, and 26.2.5.20 corresponding to ssh from 3.01 until 5.5.3, 5.2.11.7, and 5.1.4.15.	N/A	More Details
CVE-2026-41039	This vulnerability exists in Quantum Networks router due to improper access control and insecure default configuration in the web-based management interface. An unauthenticated attacker could exploit this vulnerability by accessing exposed API endpoints on the targeted device. Successful exploitation of this vulnerability could allow the attacker to access sensitive information, including internal endpoints, scripts and directories on the targeted device.	N/A	More Details
CVE-2026-41038	This vulnerability exists in Quantum Networks router due to lack of enforcement of strong password policies in the web-based management interface. An attacker on the same network could exploit this vulnerability by performing password guessing or brute-force attacks against user accounts, leading to unauthorized access to the targeted device.	N/A	More Details
CVE-2026-6553	Changing backend users' passwords via the user settings module results in storing the cleartext password in the uc and user_settings fields of the be_users database table. This issue affects TYPO3 CMS version 14.2.0.	N/A	More Details
CVE-2026-41037	This vulnerability exists in Quantum Networks router due to missing rate limiting and CAPTCHA protection for failed login attempts in the web-based management interface. An attacker on the same network could exploit this vulnerability by performing brute force attacks against administrative credentials, leading to unauthorized access with root privileges on the targeted device.	N/A	More Details
CVE-2026-41036	This vulnerability exists in Quantum Networks router due to inadequate sanitization of user-supplied input in the management CLI interface. An authenticated remote attacker could exploit this vulnerability by injecting arbitrary OS commands on the targeted device. Successful exploitation of this vulnerability could allow the attacker to perform remote code execution with root privileges on the targeted device.	N/A	More Details
CVE-	Reflected Cross-Site Scripting (XSS) vulnerability in Navigate Content Management System. The vulnerability is present in the		

2026-3317	'/blog' endpoint because user input is not properly sanitized through designed query parameters. This results in unsafe HTML rendering, which could allow a remote attacker to execute JavaScript code in the victim's browser.	N/A	More Details
CVE-2026-40496	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, attachment download tokens are generated using a weak and predictable formula: `md5(APP_KEY + attachment_id + size)`. Since attachment_id is sequential and size can be brute-forced in a small range, an unauthenticated attacker can forge valid tokens and download any private attachment without credentials. Version 1.8.213 fixes the issue.	N/A	More Details
CVE-2026-34082	Dify is an open-source LLM app development platform. Prior to 1.13.1, the method `DELETE /console/api/installed-apps/<appId>/conversations/<conversationId>` has poor authorization checking and allows any Dify-authenticated user to delete someone else's chat history. Version 1.13.1 patches the issue.	N/A	More Details
CVE-2026-40250	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.4.0 through 3.4.9, 3.3.0 through 3.3.9, and 3.2.0 through 3.2.7, `internal_dwa_compressor.h:1040` performs `chan->width * chan->bytes_per_element` in `int32` arithmetic without a `(size_t)` cast. This is the same overflow pattern fixed in other decoders by CVE-2026-34589/34588/34544, but this line was missed. Versions 3.4.10, 3.3.10, and 3.2.8 contain a fix that addresses `internal_dwa_compressor.h:1040`.	N/A	More Details
CVE-2025-10354	Cross-Site Scripting (XSS) vulnerability reflected in Semantic MediaWiki. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending them a malicious URL using the '/index.php/Speciaal:GefacetteerdZoeken' endpoint parameter. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2026-40244	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.4.0 through 3.4.9, 3.3.0 through 3.3.9, and 3.2.0 through 3.2.7, `internal_dwa_compressor.h:1722` performs `curc->width * curc->height` in `int32` arithmetic without a `(size_t)` cast. This is the same overflow pattern fixed in other locations by the recent CVE-2026-34589 batch, but this line was missed. Versions 3.4.10, 3.3.10, and 3.2.8 contain a fix that addresses `internal_dwa_compressor.h:1722`.	N/A	More Details
CVE-2026-39866	Lawnchair is a free, open-source home app for Android. Prior to commit fcba413f55dd47f8a3921445252849126c6266b2, command injection in release_update.yml workflow dispatch input allows arbitrary code execution. Commit fcba413f55dd47f8a3921445252849126c6266b2 patches the issue.	N/A	More Details
CVE-2026-40264	OpenBao is an open source identity-based secrets management system. OpenBao's namespaces provide multi-tenant separation. Prior to version 2.5.3, a tenant who leaks token accessors can have their token revoked or renewed by a privileged administrator in another tenant. This is addressed in v2.5.3.	N/A	More Details
CVE-2026-39946	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.3, when OpenBao revoked privileges on a role in the PostgreSQL database secrets engine, OpenBao failed to use proper database quoting on schema names provided by PostgreSQL. This could lead to role revocation failures, or more rarely, SQL injection as the management user. This vulnerability was original from HashiCorp Vault. The vulnerability is addressed in v2.5.3. As a workaround, audit table schemas and ensure database users cannot create new schemas and grant privileges on them.	N/A	More Details
CVE-2026-39861	Claude Code is an agentic coding tool. Prior to version 2.1.64, Claude Code's sandbox did not prevent sandboxed processes from creating symlinks pointing to locations outside the workspace. When Claude Code subsequently wrote to a path within such a symlink, its unsandboxed process followed the symlink and wrote to the target location outside the workspace without prompting the user for confirmation. This allowed a sandbox escape where neither the sandboxed command nor the unsandboxed app could independently write outside the workspace, but their combination could write to arbitrary locations, potentially leading to code execution outside the sandbox. Reliably exploiting this required the ability to add untrusted content into a Claude Code context window to trigger sandboxed code execution via prompt injection. Users on standard Claude Code auto-update have received this fix automatically. Users performing manual updates are advised to update to version 2.1.64 or later.	N/A	More Details
CVE-2026-39388	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.3, OpenBao's Certificate authentication method, when a token renewal is requested and `disable_binding=true` is set, attempts to verify the current request's presented mTLS certificate matches the original. Token renewals for other authentication methods do not require any supplied login information. Due to incorrect matching, the certificate authentication method would allow renewal of tokens for which the attacker had a sibling certificate+key signed by the same CA, but which did not necessarily match the original role or the originally supplied certificate. This implies an attacker could still authenticate to OpenBao in a similar scope, however, token renewal implies that an attacker may be able to extend the lifetime of dynamic leases held by the original token. This attack requires knowledge of either the original token or its accessor. This vulnerability is original from HashiCorp Vault. This is addressed in v2.5.3. As a workaround, ensure privileged roles are tightly scoped to single certificates.	N/A	More Details
CVE-2026-35587	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.4, a Server-Side Request Forgery (SSRF) vulnerability exists in the Glances IP plugin due to improper validation of the public_api configuration parameter. The value of public_api is used directly in outbound HTTP requests without any scheme restriction or hostname/IP validation. An attacker who can modify the Glances configuration can force the application to send requests to arbitrary internal or external endpoints. Additionally, when public_username and public_password are set, Glances automatically includes these credentials in the Authorization: Basic header, resulting in credential leakage to attacker-controlled servers. This vulnerability can be exploited to access internal network services, retrieve sensitive data from cloud metadata endpoints, and/or exfiltrate credentials via outbound HTTP requests. The issue arises because public_api is passed directly to the HTTP client (urlopen_auth) without validation, allowing unrestricted outbound connections and unintended disclosure of sensitive information. Version 4.5.4 contains a patch.	N/A	More Details
CVE-2026-34839	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.4, the Glances web server exposes a REST API (`/api/4/*`) that is accessible without authentication and allows cross-origin requests from any origin due to a permissive CORS policy (`Access-Control-Allow-Origin: *`). This allows a malicious website to read sensitive system information from a running Glances instance in the victim's browser, leading to cross-origin data exfiltration. While a previous advisory exists for XML-RPC CORS issues, this report demonstrates that the REST API (`/api/4/*`) is also affected and exposes significantly more sensitive data. Version 4.5.4 patches the issue.	N/A	More Details

CVE-2026-5958	When sed is invoked with both -i (in-place edit) and --follow-symlinks, the function open_next_file() performs two separate, non-atomic filesystem operations on the same path: 1. resolves symlink to its target and stores the resolved path for determining when output is written, 2. opens the original symlink path (not the resolved one) to read the file. Between these two calls there is a race window. If an attacker atomically replaces the symlink with a different target during that window, sed will: read content from the new (attacker-chosen) symlink target and write the processed result to the path recorded in step 1. This can lead to arbitrary file overwrite with attacker-controlled content in the context of the sed process. This issue was fixed in version 4.10.	N/A	More Details
CVE-2026-31429	In the Linux kernel, the following vulnerability has been resolved: net: skb: fix cross-cache free of KFENCE-allocated skb head SKB_SMALL_HEAD_CACHE_SIZE is intentionally set to a non-power-of-2 value (e.g. 704 on x86_64) to avoid collisions with generic kmalloc bucket sizes. This ensures that skb_kfree_head() can reliably use skb_end_offset to distinguish skb heads allocated from skb_small_head_cache vs. generic kmalloc caches. However, when KFENCE is enabled, kfence_ksize() returns the exact requested allocation size instead of the slab bucket size. If a caller (e.g. bpf_test_init) allocates skb head data via kzalloc() and the requested size happens to equal SKB_SMALL_HEAD_CACHE_SIZE, then slab_build_skb() -> ksize() returns that exact value. After subtracting skb_shared_info overhead, skb_end_offset ends up matching SKB_SMALL_HEAD_HEADROOM, causing skb_kfree_head() to incorrectly free the object to skb_small_head_cache instead of back to the original kmalloc cache, resulting in a slab cross-cache free: kmem_cache_free(skbuff_small_head): Wrong slab cache. Expected skbuff_small_head but got kmalloc-1k Fix this by always calling kfree(head) in skb_kfree_head(). This keeps the free path generic and avoids allocator-specific misclassification for KFENCE objects.	N/A	More Details
CVE-2026-32105	xrdp is an open source RDP server. In versions through 0.10.5, xrdp does not implement verification for the Message Authentication Code (MAC) signature of encrypted RDP packets when using the "Classic RDP Security" layer. While the sender correctly generates signatures, the receiving logic lacks the necessary implementation to validate the 8-byte integrity signature, causing it to be silently ignored. An unauthenticated attacker with man-in-the-middle (MITM) capabilities can exploit this missing check to modify encrypted traffic in transit without detection. It does not affect connections where the TLS security layer is enforced. This issue has been fixed in version 0.10.6. If users are unable to immediately upgrade, they should configure xrdp.ini to enforce TLS security (security_layer=tls) to ensure end-to-end integrity.	N/A	More Details
CVE-2025-13480	Fudo Enterprise in versions from 5.5.0 through 5.6.2 allows low privileged users to access certain administrator-only resources via improperly protected API endpoints. This includes sensitive information such as system logs and parts of system configuration settings. This vulnerability has been fixed in version 5.6.3	N/A	More Details
CVE-2026-40489	editorconfig-core-c is an EditorConfig core library for use by plugins supporting EditorConfig parsing. Versions up to and including 0.12.10 have a stack-based buffer overflow in ec_glob() that allows an attacker to crash any application using libeditorconfig by providing a specially crafted directory structure and .editorconfig file. This is an incomplete fix for CVE-2023-0341. The pcre_str buffer was protected in 0.12.6 but the adjacent l_pattern[8194] stack buffer received no equivalent protection. On Ubuntu 24.04, FORTIFY_SOURCE converts the overflow to SIGABRT (DoS). Version 0.12.11 contains an updated fix.	N/A	More Details
CVE-2026-40582	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the /api/public/user/login endpoint validates only the username and password before returning the user's API key, bypassing the normal authentication flow that enforces account lockout and two-factor authentication checks. An attacker with knowledge of a user's password can obtain API access even when the account is locked or has 2FA enabled, granting direct access to all protected API endpoints with that user's privileges. This issue has been fixed in version 7.2.0. Note: this issue had a duplicate, GHSA-472m-p3gf-46xp, which has been closed.	N/A	More Details
CVE-2026-40482	ChurchCRM is an open-source church management system. Versions prior to 7.2.0 have SQL injection in FinancialService::getMemberByScanString() via unsanitized $routeAndAccount concatenated into raw SQL. This issue has been fixed in version 7.2.0.	N/A	More Details
CVE-2026-40480	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the GET /api/person/{personId} endpoint loads and returns person records without performing object-level authorization checks. Although the legacy PersonView.php page enforces canEditPerson() restrictions, the API layer omits this check. Any authenticated user with only EditSelf privileges can enumerate and read other members' records, exposing sensitive PII including names, addresses, phone numbers, and email addresses. This issue has been fixed in version 7.2.0.	N/A	More Details
CVE-2026-40346	NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.37, NocoBase's workflow HTTP request plugin and custom request action plugin make server-side HTTP requests to user-provided URLs without any SSRF protection. An authenticated user can access internal network services, cloud metadata endpoints, and localhost. Version 2.0.37 contains a patch.	N/A	More Details
CVE-2026-40323	SP1 is a zero-knowledge virtual machine that proves the correct execution of programs compiled for the RISC-V architecture. In versions 6.0.0 through 6.0.2, a soundness vulnerability in the SP1 V6 recursive shard verifier allows a malicious prover to construct a recursive proof from a shard proof that the native verifier would reject. Version 6.1.0 fixes the issue.	N/A	More Details
CVE-2026-6760	Mitigation bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	N/A	More Details
CVE-2026-40481	monetr is a budgeting application for recurring expenses. In versions 1.12.3 and below, the public Stripe webhook endpoint buffers the entire request body into memory before validating the Stripe signature. A remote unauthenticated attacker can send oversized POST payloads to cause uncontrolled memory growth, leading to denial of service. The issue affects deployments with Stripe webhooks enabled and is mitigated if an upstream proxy enforces a request body size limit. This issue has been fixed in version 1.12.4.	N/A	More Details
CVE-2026-5720	miniupnpd contains an integer underflow vulnerability in SOAPAction header parsing that allows remote attackers to cause a denial of service or information disclosure by sending a malformed SOAPAction header with a single quote. Attackers can trigger an out-of-bounds memory read by exploiting improper length validation in ParseHttpHeaders(), where the parsed length underflows to a large unsigned value when passed to memchr(), causing the process to scan memory far beyond the	N/A	More Details

	allocated HTTP request buffer.		
CVE-2026-40476	graphql-go is a Go implementation of GraphQL. In versions 15.31.4 and below, the OverlappingFieldsCanBeMerged validation rule performs O(n²) pairwise comparisons of fields sharing the same response name. An attacker can send a query with thousands of repeated identical fields, causing excessive CPU usage during validation before execution begins. This is not mitigated by existing QueryDepth or QueryComplexity rules. This issue has been fixed in version 15.31.5.	N/A	More Details
CVE-2026-40353	wger is a free, open-source workout and fitness manager. In versions 2.5 and below, the attribution_link property in AbstractLicenseModel constructs HTML by directly interpolating user-controlled license fields (such as license_author) without escaping, and templates render the result using Django's |safe filter. An authenticated user can create an ingredient with a malicious license_author value containing JavaScript, which executes in the browser of any visitor viewing the ingredient page, resulting in stored XSS. This issue has been fixed in version 2.5.	N/A	More Details
CVE-2026-40306	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. All new installations of DNN 10.x.x - 10.2.1 have the same Host GUID. This does not affect upgrades from 9.x.x. Version 10.2.2 patches the issue.	N/A	More Details
CVE-2026-29013	libcoap contains out-of-bounds read vulnerabilities in OSCORE Appendix B.2 CBOR unwrap handling where get_byte_inc() in src/oscore/oscore_cbor.c relies solely on assert() for bounds checking, which is removed in release builds compiled with NDEBUG. Attackers can send crafted CoAP requests with malformed OSCORE options or responses during OSCORE negotiation to trigger out-of-bounds reads during CBOR parsing and potentially cause heap buffer overflow writes through integer wraparound in allocation size computation.	N/A	More Details
CVE-2026-40299	next-intl provides internationalization for Next.js. Applications using the `next-intl` middleware prior to version 4.9.1with `localePrefix: 'as-needed'` could construct URLs where path handling and the WHATWG URL parser resolved a relative redirect target to another host (e.g. scheme-relative `//` or control characters stripped by the URL parser), so the middleware could redirect the browser off-site while the user still started from a trusted app URL. The problem has been patchedin `next-intl@4.9.1`.	N/A	More Details
CVE-2026-40282	WeGIA is a web manager for charitable institutions. In versions prior to 3.6.10, a Stored Cross-Site Scripting (XSS) vulnerability allows an authenticated user to inject malicious JavaScript into the Intercorrências notification page, which is executed when user access the the page, enabling session hijacking and account takeover. Version 3.6.10 fixes the issue.	N/A	More Details
CVE-2026-35603	Claude Code is an agentic coding tool. In versions prior to 2.1.75 on Windows, Claude Code loaded the system-wide default configuration from C:\ProgramData\ClaudeCode\managed-settings.json without validating directory ownership or access permissions. Because the ProgramData directory is writable by non-administrative users by default and the ClaudeCode subdirectory was not pre-created or access-restricted, a low-privileged local user could create this directory and place a malicious configuration file that would be automatically loaded for any user launching Claude Code on the same machine. Exploiting this would have required a shared multi-user Windows system and a victim user to launch Claude Code after the malicious configuration was placed. This issue has been fixed on version 2.1.75.	N/A	More Details
CVE-2026-35512	xrdp is an open source RDP server. Versions through 0.10.5 have a heap-based buffer overflow in the EGFX (graphics dynamic virtual channel) implementation due to insufficient validation of client-controlled size parameters, allowing an out-of-bounds write via crafted PDUs. Pre-authentication exploitation can crash the process, while post-authentication exploitation may achieve remote code execution. This issue has been fixed in version 0.10.6. If users are unable to immediately update, they should run xrdp as a non-privileged user (default since 0.10.2) to limit the impact of successful exploitation.	N/A	More Details
CVE-2026-35402	mcp-neo4j-cypher is an MCP server for executing Cypher queries against Neo4j databases. In versions prior to 0.6.0, the read_only mode enforcement can be bypassed using APOC CALL procedures, potentially allowing unauthorized write operations or server-side request forgery. This issue is fixed in version 0.6.0.	N/A	More Details
CVE-2026-33689	xrdp is an open source RDP server. Versions through 0.10.5 have an out-of-bounds read vulnerability in the pre-authentication RDP message parsing logic. A remote, unauthenticated attacker can trigger this flaw by sending a specially crafted sequence of packets during the initial connection phase. This vulnerability results from insufficient validation of input buffer lengths before processing dynamic channel communication. Successful exploitation can lead to a denial-of-service (DoS) condition via a process crash or potential disclosure of sensitive information from the service's memory space. This issue has been fixed in version 0.10.6.	N/A	More Details
CVE-2026-23500	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. In versions prior to 23.0.0 , the ODT to PDF conversion process in odf.php concatenates the MAIN_ODT_AS_PDF configuration constant directly into a shell command passed to exec() without sanitization. An authenticated administrator can inject arbitrary OS commands via this constant using command separators, achieving remote code execution as the web server user when any ODT template is generated. This issue has been fixed in version 23.0.0.	N/A	More Details
CVE-2026-33516	xrdp is an open source RDP server. Versions through 0.10.5 contain an out-of-bounds read vulnerability during the RDP capability exchange phase. The issue occurs when memory is accessed before validating the remaining buffer length. A remote, unauthenticated attacker can trigger this vulnerability by sending a specially crafted Confirm Active PDU. Successful exploitation could lead to a denial of service (process crash) or potential disclosure of sensitive information from the process memory. This issue has been fixed in version 0.10.6.	N/A	More Details
CVE-2026-32624	xrdp is an open source RDP server. Versions through 0.10.5 contain a heap-based buffer overflow vulnerability in its logon processing. In environments where domain_user_separator is configured in xrdp.ini, an unauthenticated remote attacker can send a crafted, excessively long username and domain name to overflow the internal buffer. This can corrupt adjacent memory regions, potentially leading to a Denial of Service (DoS) or unexpected behavior. The domain_name_separator directive is commented out by default, systems are not affected by this vulnerability unless it is intentionally configured. This issue has been fixed in version 0.10.6.	N/A	More Details
CVE-	xrdp is an open source RDP server. Versions through 0.10.5 contain a heap-based buffer overflow vulnerability in the NeutrinoRDP module. When proxying RDP sessions from xrdp to another server, the module fails to properly validate the size of reassembled fragmented virtual channel data against its allocated memory buffer. A malicious downstream RDP server (or		

2026-32623	an attacker capable of performing a Man-in-the-Middle attack) could exploit this flaw to cause memory corruption, potentially leading to a Denial of Service (DoS) or Remote Code Execution (RCE). The NeutrinoRDP module is not built by default. This vulnerability only affects environments where the module has been explicitly compiled and enabled. Users can verify if the module is built by checking for --enable-neutrinordp in the output of the xrdp -v command. This issue has been fixed in version 0.10.6.	N/A	More Details
CVE-2025-70420	A SQL injection vulnerability exists in Genesys Latitude v25.1.0.420 that allows an authenticated attacker to execute arbitrary SQL queries against the backend database. The vulnerability is caused by unsanitized user-supplied input being concatenated directly into SQL statements.	N/A	More Details
CVE-2026-41242	protobufjs compiles protobuf definitions into JavaScript (JS) functions. In versions prior to 8.0.1 and 7.5.5, attackers can inject arbitrary code in the "type" fields of protobuf definitions, which will then execute during object decoding using that definition. Versions 8.0.1 and 7.5.5 patch the issue.	N/A	More Details
CVE-2026-6056	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-32963	SD-330AC and AMC Manager provided by silex technology, Inc. contain a reflected cross-site scripting vulnerability. When a user logs in to the affected device and access some crafted web page, arbitrary script may be executed on the user's browser.	N/A	More Details
CVE-2026-39454	SKYSEA Client View and SKYMEC IT Manager provided by Sky Co.,LTD. configure the installation folder with improper file access permission settings. A non-administrative user may manipulate and/or place arbitrary files within the installation folder of the product. As a result, arbitrary code may be executed with the administrative privilege.	N/A	More Details
CVE-2026-40599	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. Prior to 5.0.5, ClearanceKit incorrectly treats a process with an empty Team ID and a non-empty Signing ID as an Apple platform binary. This bug allows a malicious software to impersonate an apple process in the global allowlist, and access all protected files. This vulnerability is fixed in 5.0.5.	N/A	More Details
CVE-2026-40604	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. Prior to 5.0.6, the opfilter Endpoint Security system extension (bundle ID uk.craigbass.clearancekit.opfilter) can be suspended with SIGSTOP or kill -STOP, or killed with SIGKILL/SIGTERM, by any process running as root. While the extension is suspended, all AUTH Endpoint Security events time out and default to allow, silently disabling ClearanceKit's file-access policy enforcement for the duration of the suspension. This vulnerability is fixed in 5.0.6.	N/A	More Details
CVE-2026-6644	A command injection vulnerability was found in the PPTP VPN Clients on the ADM. The vulnerability allows an administrative user to break out of the restricted web environment and execute arbitrary code on the underlying operating system. This occurs due to insufficient validation of user-supplied input before it is passed to a system shell. Successful exploitation allows an attacker to achieve Remote Code Execution (RCE) and fully compromise the system. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RR42 as well as from ADM 5.0.0 through ADM 5.1.2.REO1.	N/A	More Details
CVE-2026-6643	A stack-based buffer overflow vulnerability was found in the VPN Clients on the ADM. The issue stems from the use of unbounded sscanf() and passing user-controlled data directly to printf(). Due to the lack of PIE and Stack Canary protections, an authenticated remote attacker can exploit these to execute arbitrary code as the web server user. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RR42 as well as from ADM 5.0.0 through ADM 5.1.2.REO1.	N/A	More Details
CVE-2026-40614	PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, there is a buffer overflow when decoding Opus audio frames due to insufficient buffer size validation in the Opus codec decode path. The FEC decode buffers (dec_frame[].buf) were allocated based on a PCM-derived formula: (sample_rate/1000) * 60 * channel_cnt * 2. At 8 kHz mono this yields only 960 bytes, but codec_parse() can output encoded frames up to MAX_ENCODED_PACKET_SIZE (1280) bytes via opus_repacketizer_out_range(). The three pj_memcpy() calls in codec_decode() copied input->size bytes without bounds checking, causing a heap buffer overflow.	N/A	More Details
CVE-2026-40865	Horilla is a free and open source Human Resource Management System (HRMS). In 1.5.0, an insecure direct object reference in the employee document viewer allows any authenticated user to access other employees' uploaded documents by changing the document ID in the request. This exposes sensitive HR files such as identity documents, contracts, certificates, and other private employee records.	N/A	More Details
CVE-2026-40866	Horilla is a free and open source Human Resource Management System (HRMS). In 1.5.0, an insecure direct object reference in the employee document upload endpoint allows any authenticated user to overwrite or replace or corrupt another employee's document by changing the document ID in the upload request. This enables unauthorized modification of HR records.	N/A	More Details
CVE-2026-40867	Horilla is a free and open source Human Resource Management System (HRMS). In 1.5.0, a broken access control vulnerability in the helpdesk attachment viewer allows any authenticated user to view attachments from other tickets by changing the attachment ID. This can expose sensitive support files and internal documents across unrelated users or teams.	N/A	More Details
CVE-2026-41456	Bludit CMS prior to commit 6732dde contains a reflected cross-site scripting vulnerability in the search plugin that allows unauthenticated attackers to inject arbitrary JavaScript by crafting a malicious search query. Attackers can execute malicious scripts in the browsers of users who visit crafted URLs containing the payload, potentially stealing session cookies or performing actions on behalf of affected users.	N/A	More Details
CVE-2026-33813	Parsing a WEBP image with an invalid, large size panics on 32-bit platforms.	N/A	More Details
CVE-2026-40888	Frappe HR is an open-source human resources management solution (HRMS). Prior to versions 15.58.1 and 16.4.1, an authenticated user with default role can access unauthorized information by exploiting certain api endpoint. Versions 15.58.1 and 16.4.1 contain a patch. No known workarounds are available.	N/A	More Details

CVE-2026-40872	mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, the admin dashboard's Autodiscover logs render the EMailAddress value (logged as the "user" field) without HTML escaping. By submitting an unauthenticated Autodiscover request with a crafted EMailAddress containing HTML/JS, the payload is stored in Redis and executed when an admin views the Autodiscover logs. Version 2026-03b fixes the vulnerability.	N/A	More Details
CVE-2026-40873	mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, the Quarantine details modal injects attachment filenames into HTML without escaping, allowing arbitrary HTML/JS execution. An attacker can deliver an email with a crafted attachment name so that when an admin views the quarantine item, JavaScript executes in their browser, taking over their account. Version 2026-03b fixes the vulnerability.	N/A	More Details
CVE-2026-40874	mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, no administrator verification takes place when deleting Forwarding Hosts with `/api/v1/delete/fwdhost`. Any authenticated user can call this API. Checks are only applied for edit/add actions, but deletion can still significantly disrupt the mail service. Version 2026-03b fixes the vulnerability.	N/A	More Details
CVE-2026-40875	mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, the user dashboard's "Seen successful connections" (login history) renders the client IP from login logs without HTML escaping. Because the server trusts the X-Real-IP header as the source IP for logging, an attacker can inject HTML/JS into this field. This Self-XSS can be exploited by a Login CSRF to force the victim into the attacker's account, and then read emails in a previous browser tab. Version 2026-03b fixes the vulnerability.	N/A	More Details
CVE-2026-40876	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.6, goshs contains an SFTP root escape caused by prefix-based path validation. An authenticated SFTP user can read from and write to filesystem paths outside the configured SFTP root, which breaks the intended jail boundary and can expose or modify unrelated server files. The SFTP subsystem routes requests through sftpserver/sftpserver.go into DefaultHandler.GetHandler() in sftpserver/handler.go, which forwards file operations into readFile, writeFile, listFile, and cmdFile. All of those sinks rely on sanitizePath() in sftpserver/helper.go. helper.go uses a raw string-prefix comparison, not a directory-boundary check. Because of that, if the configured root is /tmp/goshsroot, then a sibling path such as /tmp/goshsroot_evil/secret.txt incorrectly passes validation since it starts with the same byte prefix. This vulnerability is fixed in 2.0.0-beta.6.	N/A	More Details
CVE-2026-40878	mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, the mailcow web interface passes the raw `$_SERVER['REQUEST_URI']` to Twig as a global template variable and renders it inside a JavaScript string literal in the `setLang()` helper of `base.twig`, relying on Twig's default HTML auto-escaping instead of the context-appropriate `js` escaping strategy. In addition, the `query_string()` Twig helper merges all current `$_GET` parameters into the language-switching links on the login page, so attacker-supplied parameters are reflected and preserved across navigation. Version 2026-03b fixes the vulnerability.	N/A	More Details
CVE-2026-40880	ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.1 and zebra-consensus version 5.0.2, a logic error in Zebra's transaction verification cache could allow a malicious miner to induce a consensus split. By carefully submitting a transaction that is valid for height H+1 but invalid for H+2 and then mining that transaction in a block at height H+2, a miner could cause vulnerable Zebra nodes to accept an invalid block, leading to a consensus split from the rest of the Zcash network. This vulnerability is fixed in zebrad version 4.3.1 and zebra-consensus version 5.0.2.	N/A	More Details
CVE-2026-40881	ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.0 and zebra-network version 5.0.1, when deserializing addr or addrv2 messages, which contain vectors of addresses, Zebra would fully deserialize them up to a maximum length (over 233,000) that was derived from the 2 MiB message size limit. This is much larger than the actual limit of 1,000 messages from the specification. Zebra would eventually check that limit but, at that point, the memory for the larger vector was already allocated. An attacker could cause out-of-memory aborts in Zebra by sending multiple such messages over different connections. This vulnerability is fixed in zebrad version 4.3.0 and zebra-network version 5.0.1.	N/A	More Details
CVE-2026-40883	goshs is a SimpleHTTPServer written in Go. From 2.0.0-beta.4 to 2.0.0-beta.5, goshs contains a cross-site request forgery issue in its state-changing HTTP GET routes. An external attacker can cause an already authenticated browser to trigger destructive actions such as ?delete and ?mkdir because goshs relies on HTTP basic auth alone and performs no CSRF, Origin, or Referer validation for those routes. This vulnerability is fixed in 2.0.0-beta.6.	N/A	More Details
CVE-2026-40885	goshs is a SimpleHTTPServer written in Go. From 2.0.0-beta.4 to 2.0.0-beta.5, goshs leaks file-based ACL credentials through its public collaborator feed when the server is deployed without global basic auth. Requests to .goshs-protected folders are logged before authorization is enforced, and the collaborator websocket broadcasts raw request headers, including Authorization. An unauthenticated observer can capture a victim's folder-specific basic-auth header and replay it to read, upload, overwrite, and delete files inside the protected subtree. This vulnerability is fixed in 2.0.0-beta.6.	N/A	More Details
CVE-2026-5921	A server-side request forgery (SSRF) vulnerability was identified in GitHub Enterprise Server that allowed an attacker to extract sensitive environment variables from the instance through a timing side-channel attack against the notebook rendering service. When private mode was disabled, the notebook viewer followed HTTP redirects without revalidating the destination host, enabling an unauthenticated SSRF to internal services. By chaining this with regex filter queries against an internal API and measuring response time differences, an attacker could infer secret values character by character. Exploitation required that private mode be disabled and that the attacker be able to chain the instance's open redirect endpoint through an external redirect to reach internal services. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21 and was fixed in versions 3.14.26, 3.15.21, 3.16.17, 3.17.14, 3.18.8, 3.19.5, and 3.20.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details