SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 March 2026

Generated on 04 March 2026

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-28289	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. A patch bypass vulnerability for CVE-2026-27636 in FreeScout 1.8.206 and earlier allows any authenticated user with file upload permissions to achieve Remote Code Execution (RCE) on the server by uploading a malicious .htaccess file using a zero-width space character prefix to bypass the security check. The vulnerability exists in the sanitizeUploadedFileName() function in app/Http/Helper.php. The function contains a Time-of-Check to Time-of-Use (TOCTOU) flaw where the dot-prefix check occurs before sanitization removes invisible characters. This vulnerability is fixed in 1.8.207.	10.0	More Details
CVE-2026-24898	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0, an unauthenticated token disclosure vulnerability in the MedEx callback endpoint allows any unauthenticated visitor to obtain the practice's MedEx API tokens, leading to complete third-party service compromise, PHI exfiltration, unauthorized actions on the MedEx platform, and HIPAA violations. The vulnerability exists because the endpoint bypasses authentication ($ignoreAuth = true) and performs a MedEx login whenever $_POST['callback_key'] is provided, returning the full JSON response including sensitive API tokens. This vulnerability is fixed in 8.0.0.	10.0	More Details
CVE-2026-28409	WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, a critical Remote Code Execution (RCE) vulnerability exists in the WeGIA application's database restoration functionality. An attacker with administrative access (which can be obtained via the previously reported Authentication Bypass) can execute arbitrary OS commands on the server by uploading a backup file with a specifically crafted filename. Version 3.6.5 fixes the issue.	10.0	More Details
CVE-2026-27597	Enclave is a secure JavaScript sandbox designed for safe AI agent code execution. Prior to version 2.11.1, it is possible to escape the security boundraries set by `@enclave-vm/core`, which can be used to achieve remote code execution (RCE). The issue has been fixed in version 2.11.1.	10.0	More Details
CVE-2026-	An authentication bypass vulnerability exists in Copeland XWEB Pro version 1.12.1 and prior,		More

21718	enabling any attackers to bypass the authentication requirement and achieve pre-authenticated code execution on the system.	10.0	Details
CVE-2026-20127	A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system. This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to an affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.	10.0	More Details
CVE-2026-27702	Budibase is a low code platform for creating internal tools, workflows, and admin panels. Prior to version 3.30.4, an unsafe `eval()` vulnerability in Budibase's view filtering implementation allows any authenticated user (including free tier accounts) to execute arbitrary JavaScript code on the server. This vulnerability ONLY affects Budibase Cloud (SaaS) - self-hosted deployments use native CouchDB views and are not vulnerable. The vulnerability exists in `packages/server/src/db/inMemoryView.ts` where user-controlled view map functions are directly evaluated without sanitization. The primary impact comes from what lives inside the pod's environment: the `app-service` pod runs with secrets baked into its environment variables, including `INTERNAL_API_KEY`, `JWT_SECRET`, CouchDB admin credentials, AWS keys, and more. Using the extracted CouchDB credentials, we verified direct database access, enumerated all tenant databases, and confirmed that user records (email addresses) are readable. Version 3.30.4 contains a patch.	9.9	More Details
CVE-2026-2749	Vulnerability in Centreon Centreon Open Tickets on Central Server on Linux (Centroen Open Ticket modules).This issue affects Centreon Open Tickets on Central Server: from all before 25.10.3, 24.10.8, 24.04.7.	9.9	More Details
CVE-2026-28363	In OpenClaw before 2026.2.23, tools.exec.safeBins validation for sort could be bypassed via GNU long-option abbreviations (such as --compress-prog) in allowlist mode, leading to approval-free execution paths that were intended to require approval. Only an exact string such as --compress-program was denied.	9.9	More Details
CVE-2026-27965	Vitess is a database clustering system for horizontal scaling of MySQL. Prior to versions 23.0.3 and 22.0.4, anyone with read/write access to the backup storage location (e.g. an S3 bucket) can manipulate backup manifest files so that arbitrary code is later executed when that backup is restored. This can be used to provide that attacker with unintended/unauthorized access to the production deployment environment — allowing them to access information available in that environment as well as run any additional arbitrary commands there. Versions 23.0.3 and 22.0.4 contain a patch. Some workarounds are available. Those who intended to use an external decompressor then can always specify that decompressor command in the `--external-decompressor` flag value for `vttablet` and `vtbackup`. That then overrides any value specified in the manifest file. Those who did not intend to use an external decompressor, nor an internal one, can specify a value such as `cat` or `tee` in the `--external-decompressor` flag value for `vttablet` and `vtbackup` to ensure that a harmless command is always used.	9.9	More Details
CVE-2026-27941	OpenLIT is an open source platform for AI engineering. Prior to version 1.37.1, several GitHub Actions workflows in OpenLIT's GitHub repository use the `pull_request_target` event while checking out and executing untrusted code from forked pull requests. These workflows run with the security context of the base repository, including a write-privileged `GITHUB_TOKEN` and numerous sensitive secrets (API keys, database/vector store tokens, and a Google Cloud service account key). Version 1.37.1 contains a fix.	9.9	More Details
CVE-2026-24908	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, an SQL injection vulnerability in the Patient REST API endpoint allows authenticated users with API access to execute arbitrary SQL queries through the `_sort` parameter. This could potentially lead to database access, PHI (Protected Health Information) exposure, and credential compromise. The issue occurs when user-supplied sort field names are used in ORDER BY clauses without proper validation or identifier escaping. Version 8.0.0 fixes the issue.	9.9	More Details
	OneUptime is a solution for monitoring and managing online services. Prior to version 10.0.7,		

CVE-2026-27728	an OS command injection vulnerability in `NetworkPathMonitor.performTraceroute()` allows any authenticated project user to execute arbitrary operating system commands on the Probe server by injecting shell metacharacters into a monitor's destination field. Version 10.0.7 fixes the vulnerability.	9.9	More Details
CVE-2026-24849	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 7.0.4, the `disposeDocument()` method in `EtherFaxActions.php` allows authenticated users to read arbitrary files from the server filesystem. Any authenticated user (regardless of privilege level) can exploit this vulnerability to read sensitive files. Version 7.0.4 patches the issue.	9.9	More Details
CVE-2026-27626	OliveTin gives access to predefined shell commands from a web interface. In versions up to and including 3000.10.0, OliveTin's shell mode safety check (`checkShellArgumentSafety`) blocks several dangerous argument types but not `password`. A user supplying a `password`-typed argument can inject shell metacharacters that execute arbitrary OS commands. A second independent vector allows unauthenticated RCE via webhook-extracted JSON values that skip type safety checks entirely before reaching `sh -c`. When exploiting vector 1, any authenticated user (registration enabled by default, `authType: none` by default) can execute arbitrary OS commands on the OliveTin host with the permissions of the OliveTin process. When exploiting vector 2, an unauthenticated attacker can achieve the same if the instance receives webhooks from external sources, which is a primary OliveTin use case. When an attacker exploits both vectors, this results in unauthenticated RCE on any OliveTin instance using Shell mode with webhook-triggered actions. As of time of publication, a patched version is not available.	9.9	More Details
CVE-2025-62878	A malicious user can manipulate the parameters.pathPattern to create PersistentVolumes in arbitrary locations on the host node, potentially overwriting sensitive files or gaining access to unintended directories.	9.9	More Details
CVE-2026-28408	WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, the script in adicionar_tipo_docs_atendido.php does not go through the project's central controller and does not have its own authentication and permission checks. A malicious user could make a request through tools like Postman or the file's URL on the web to access features exclusive to employees. The vulnerability allows external parties to inject unauthorized data in massive quantities into the application server's storage. Version 3.6.5 fixes the issue.	9.8	More Details
CVE-2026-24109	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by controlling the value of `picName`. When this value is used in `sprintf` without validating variable sizes, it could lead to a buffer overflow vulnerability.	9.8	More Details
CVE-2025-52998	Chamilo is a learning management system. Prior to version 1.11.30, in the application, deserialization of data is performed, the data can be spoofed. An attacker can create objects of arbitrary classes, as well as fully control their properties, and thus modify the logic of the web application's operation. This issue has been patched in version 1.11.30.	9.8	More Details
CVE-2026-26703	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/advance_search.php.	9.8	More Details
CVE-2026-26702	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/myitem_reuse.php.	9.8	More Details
CVE-2026-26696	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_edit.php.	9.8	More Details
CVE-2026-26695	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordstudent_edit.php.	9.8	More Details
CVE-2026-26694	code-projects Simple Student Alumni System v1.0 is vulnerale to SQL Injection in /TracerStudy/modal_view.php.	9.8	More Details
CVE-2026-24115	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate the sizes of `gstup` and `gstdwn` before concatenating them into `gstruleQos` may lead to buffer overflow.	9.8	More Details
CVE-2026-24114	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate `pPortMapIndex` may lead to buffer overflows when using `strcpy`.	9.8	More Details

CVE-2026-24113	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by controlling the value of `nptr`. When this value is passed into the `getMibPrefix` function and concatenated using `sprintf` without proper size validation, it could lead to a buffer overflow vulnerability.	9.8	More Details
CVE-2026-24111	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by specifying the value of `userInfo`. When `userInfo` is passed into the `addAuthUser` function and processed by `sscanf` without size validation, it could lead to buffer overflow.	9.8	More Details
CVE-2026-24108	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by controlling the value of `nptr`. When this value is passed into the `getMibPrefix` function and concatenated using `sprintf` without proper size validation, it could lead to a buffer overflow vulnerability.	9.8	More Details
CVE-2026-24110	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may send overly long `addDhcpRules` data. When these rules enter the `addDhcpRule` function and are processed by `ret = sscanf(pRule, " %d\t%[^\t]\t%[^\n\r\t]", &dhcpsIndex, dhcpsIP, dhcpsMac);`, the lack of size validation for the rules could lead to buffer overflows in `dhcpsIndex`, `dhcpsIP`, and `dhcpsMac`.	9.8	More Details
CVE-2026-24107	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate the value of `usbPartitionName`, which is directly used in `doSystemCmd`, may lead to critical command injection vulnerabilities.	9.8	More Details
CVE-2025-50192	Chamilo is a learning management system. Prior to version 1.11.30, there is a time-based SQL Injection in found in /main/webservices/registration.soap.php. This issue has been patched in version 1.11.30.	9.8	More Details
CVE-2025-50190	Chamilo is a learning management system. Prior to version 1.11.30, there is an error-based SQL Injection via the GET openid.assoc_handle parameter with the /index.php script. This issue has been patched in version 1.11.30.	9.8	More Details
CVE-2025-50187	Chamilo is a learning management system. Prior to version 1.11.28, parameter from SOAP request is evaluated without filtering which leads to Remote Code Execution. This issue has been patched in version 1.11.28.	9.8	More Details
CVE-2026-3431	On SimStudio version below to 0.5.74, the MongoDB tool endpoints accept arbitrary connection parameters from the caller without authentication or host restrictions. An attacker can leverage these endpoints to connect to any reachable MongoDB instance and perform unauthorized operations including reading, modifying, and deleting data.	9.8	More Details
CVE-2026-3422	U-Office Force developed by e-Excellence has a Insecure Deserialization vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server by sending maliciously crafted serialized content.	9.8	More Details
CVE-2026-3000	IDExpert Windows Logon Agent developed by Changing has a Remote Code Execution vulnerability, allowing unauthenticated remote attackers to force the system to download arbitrary DLL files from a remote source and execute them.	9.8	More Details
CVE-2026-2999	IDExpert Windows Logon Agent developed by Changing has a Remote Code Execution vulnerability, allowing unauthenticated remote attackers to force the system to download arbitrary executable files from a remote source and execute them.	9.8	More Details
CVE-2026-28411	WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, an unsafe use of the `extract()` function on the `$_REQUEST` superglobal allows an unauthenticated attacker to overwrite local variables in multiple PHP scripts. This vulnerability can be leveraged to completely bypass authentication checks, allowing unauthorized access to administrative and protected areas of the WeGIA application. Version 3.6.5 fixes the issue.	9.8	More Details
CVE-2026-24101	An issue was discovered in goform/formSetIptv in Tenda AC15V1.0 V15.03.05.18_multi. When the condition is met, `s1_1` will be passed into sub_B0488, concatenated into `doSystemCmd`. The value of s1_1 is not validated, potentially leading to a command injection vulnerability.	9.8	More Details
CVE-2026-24112	An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by specifying the value of `userInfo`. When `userInfo` is passed into the `addWewifiWhiteUser` function and processed by `sscanf` without size validation, it could lead	9.8	More Details

	to a buffer overflow vulnerability.		
CVE-2026-27755	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a weak session identifier generation vulnerability that allows attackers to forge authenticated sessions by computing predictable MD5-based cookies. Attackers who know or guess valid credentials can calculate the session identifier offline and bypass authentication without completing the login flow, gaining unauthorized access to the device.	9.8	More Details
CVE-2026-26701	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_tecnical_user.php.	9.8	More Details
CVE-2026-27012	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, a privilege escalation and authentication bypass vulnerability in OpenSTAManager allows any attacker to arbitrarily change a user's group (idgruppo) by directly calling modules/utenti/actions.php. This can promote an existing account (e.g. agent) into the Amministratori group as well as demote any user including existing administrators.	9.8	More Details
CVE-2026-3485	A flaw has been found in D-Link DIR-868L 110b03. This affects the function sub_1BF84 of the component SSDP Service. This manipulation of the argument ST causes os command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-55020	A command injection vulnerability in the DHCP activation feature of Weintek cMT-3072XH2 easyweb Web Version v2.1.53, OS v20231011 allows attackers to execute arbitrary commands with root privileges.	9.8	More Details
CVE-2026-22891	A heap-based buffer overflow vulnerability exists in the Intan CLP parsing functionality of The Biosig Project libbiosig 3.9.2 and Master Branch (db9a9a63). A specially crafted Intan CLP file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-59059	Remote Code Execution Vulnerability in NashornScriptEngineCreator is reported in Apache Ranger versions <= 2.7.0. Users are recommended to upgrade to version 2.8.0, which fixes this issue.	9.8	More Details
CVE-2026-22886	OpenMQ exposes a TCP-based management service (imqbrokerd) that by default requires authentication. However, the product ships with a default administrative account (admin/ admin) and does not enforce a mandatory password change on first use. After the first successful login, the server continues to accept the default password indefinitely without warning or enforcement. In real-world deployments, this service is often left enabled without changing the default credentials. As a result, a remote attacker with access to the service port could authenticate as an administrator and gain full control of the protocol’s administrative features.	9.8	More Details
CVE-2026-1492	The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to improper privilege management in all versions up to, and including, 5.1.2. This is due to the plugin accepting a user-supplied role during membership registration without properly enforcing a server-side allowlist. This makes it possible for unauthenticated attackers to create administrator accounts by supplying a role value during membership registration.	9.8	More Details
CVE-2026-2628	The All-in-One Microsoft 365 & Entra ID / Azure AD SSO Login plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.2.5. This makes it possible for unauthenticated attackers to bypass authentication and log in as other users, including administrators.	9.8	More Details
CVE-2026-26713	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/cancel-order.php.	9.8	More Details
CVE-2026-26712	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket-admin.php.	9.8	More Details
CVE-2026-26711	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket.php.	9.8	More Details
CVE-2026-26710	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/edit-orders.php.	9.8	More Details

CVE-2026-0006	In multiple locations, there is a possible out of bounds read and write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2026-26707	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_supplier.php.	9.8	More Details
CVE-2026-26706	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_receipt.php.	9.8	More Details
CVE-2026-26705	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_product.php.	9.8	More Details
CVE-2026-26704	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_category.php.	9.8	More Details
CVE-2026-26708	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_user.php.	9.8	More Details
CVE-2026-26700	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_employee.php.	9.8	More Details
CVE-2026-24105	An issue was discovered in goform/formsetUsbUnload in Tenda AC15V1.0 V15.03.05.18_multi. The value of `v1` was not checked, potentially leading to a command injection vulnerability if injected into doSystemCmd.	9.8	More Details
CVE-2026-26720	An issue in Twenty CRM v1.15.0 and before allows a remote attacker to execute arbitrary code via the local.driver.ts module.	9.8	More Details
CVE-2026-28268	Vikunja is an open-source self-hosted task management platform. Versions prior to 2.1.0 have a business logic vulnerability exists in the password reset mechanism of vikunja/api that allows password reset tokens to be reused indefinitely. Due to a failure to invalidate tokens upon use and a critical logic bug in the token cleanup cron job, reset tokens remain valid forever. This allows an attacker who intercepts a single reset token (via logs, browser history, or phishing) to perform a complete, persistent account takeover at any point in the future, bypassing standard authentication controls. Version 2.1.0 contains a patch for the issue.	9.8	More Details
CVE-2026-24352	PluXml CMS allows a user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behaviour enables an attacker to fix a session ID for a victim and later hijack the authenticated session. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 5.8.21 and 5.9.0-rc7 were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	9.8	More Details
CVE-2026-27751	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a default credentials vulnerability that allows remote attackers to obtain administrative access to the management interface. Attackers can authenticate using the hardcoded default credentials without password change enforcement to gain full administrative control of the device.	9.8	More Details
CVE-2026-25955	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_AppUpdateWindowFromSurface` reuses a cached `XImage` whose `data` pointer references a freed RDPGFX surface buffer, because `gdi_DeleteSurface` frees `surface->data` without invalidating the `appWindow->image` that aliases it. Version 3.23.0 fixes the issue.	9.8	More Details
CVE-2025-50857	ZenTaoPMS v18.11 through v21.6.beta is vulnerable to Directory Traversal in /module/ai/control.php. This allows attackers to execute arbitrary code via a crafted file upload	9.8	More Details
CVE-2026-27975	Ajenti is a Linux and BSD modular server admin panel. Prior to version 2.2.13, an unauthenticated user could gain access to a server to execute arbitrary code on this server. This is fixed in the version 2.2.13.	9.8	More Details
CVE-2026-27966	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.8.0, the CSV Agent node in Langflow hardcodes `allow_dangerous_code=True`, which automatically exposes LangChain’s Python REPL tool (`python_repl_ast`). As a result, an attacker can execute arbitrary Python and OS commands on the server via prompt injection, leading to full Remote Code Execution (RCE). Version 1.8.0 fixes the issue.	9.8	More Details

CVE-2026-27743	The SPIP referer_spam plugin versions prior to 1.3.0 contain an unauthenticated SQL injection vulnerability in the referer_spam_ajouter and referer_spam_supprimer action handlers. The handlers read the url parameter from a GET request and interpolate it directly into SQL LIKE clauses without input validation or parameterization. The endpoints do not enforce authorization checks and do not use SPIP action protections such as securiser_action(), allowing remote attackers to execute arbitrary SQL queries.	9.8	More Details
CVE-2026-27744	The SPIP tickets plugin versions prior to 4.3.3 contain an unauthenticated remote code execution vulnerability in the forum preview handling for public ticket pages. The plugin appends untrusted request parameters into HTML that is later rendered by a template using unfiltered environment rendering (#ENV**), which disables SPIP output filtering. As a result, an unauthenticated attacker can inject crafted content that is evaluated through SPIP's template processing chain, leading to execution of code in the context of the web server.	9.8	More Details
CVE-2026-25997	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_clipboard_format_equal` reads freed `lastSentFormats` memory because `xf_clipboard_formats_free` (called from the cliprdr channel thread during auto-reconnect) frees the array while the X11 event thread concurrently iterates it in `xf_clipboard_changed`, triggering a heap use after free. Version 3.23.0 fixes the issue.	9.8	More Details
CVE-2026-25959	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_cliprdr_provide_data_` passes freed `pDstData` to `XChangeProperty` because the cliprdr channel thread calls `xf_cliprdr_server_format_data_response` which converts and uses the clipboard data without holding any lock, while the X11 event thread concurrently calls `xf_cliprdr_clear_cached_data` → `HashTable_Clear` which frees the same data via `xf_cached_data_free`, triggering a heap use after free. Version 3.23.0 fixes the issue.	9.8	More Details
CVE-2026-25953	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_AppUpdateWindowFromSurface` reads from a freed `xfAppWindow` because the RDPGFX DVC thread obtains a bare pointer via `xf_rail_get_window` without any lifetime protection, while the main thread can concurrently delete the window through a fastpath window-delete order. Version 3.23.0 fixes the issue.	9.8	More Details
CVE-2026-27641	Flask-Reuploaded provides file uploads for Flask. A critical path traversal and extension bypass vulnerability in versions prior to 1.5.0 allows remote attackers to achieve arbitrary file write and remote code execution through Server-Side Template Injection (SSTI). Flask-Reuploaded has been patched in version 1.5.0. Some workarounds are available. Do not pass user input to the `name` parameter, use auto-generated filenames only, and implement strict input validation if `name` must be used.	9.8	More Details
CVE-2026-25952	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_SetWindowMinMaxInfo` dereferences a freed `xfAppWindow` pointer because `xf_rail_get_window` in `xf_rail_server_min_max_info` returns an unprotected pointer from the `railWindows` hash table, and the main thread can concurrently delete the window (via a window delete order) while the RAIL channel thread is still using the pointer. Version 3.23.0 fixes the issue.	9.8	More Details
CVE-2026-21902	An Incorrect Permission Assignment for Critical Resource vulnerability in the On-Box Anomaly detection framework of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated, network-based attacker to execute code as root. The On-Box Anomaly detection framework should only be reachable by other internal processes over the internal routing instance, but not over an externally exposed port. With the ability to access and manipulate the service to execute code as root a remote attacker can take complete control of the device. Please note that this service is enabled by default as no specific configuration is required. This issue affects Junos OS Evolved on PTX Series: * 25.4 versions before 25.4R1-S1-EVO, 25.4R2-EVO. This issue does not affect Junos OS Evolved versions before 25.4R1-EVO. This issue does not affect Junos OS.	9.8	More Details
CVE-2026-27849	Due to missing neutralization of special elements, OS commands can be injected via the update functionality of a TLS-SRP connection, which is normally used for configuring devices inside the mesh network. This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	9.8	More Details
CVE-2026-	A vulnerability in the API user authentication of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain access to an affected system as a user who has the netadmin role. The vulnerability is due to improper authentication for requests that		More

20129	are sent to the API. An attacker could exploit this vulnerability by sending a crafted request to the API of an affected system. A successful exploit could allow the attacker to execute commands with the privileges of the netadmin role. Note: Cisco Catalyst SD-WAN Manager releases 20.18 and later are not affected by this vulnerability.	9.8	Details
CVE-2026-2624	Missing Authentication for Critical Function vulnerability in ePati Cyber Security Technologies Inc. Antikor Next Generation Firewall (NGFW) allows Authentication Bypass.This issue affects Antikor Next Generation Firewall (NGFW): from v.2.0.1298 before v.2.0.1301.	9.8	More Details
CVE-2026-27848	Due to missing neutralization of special elements, OS commands can be injected via the handshake of a TLS-SRP connection, which are ultimately run as the root user. This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	9.8	More Details
CVE-2026-27847	Due to improper neutralization of special elements, SQL statements can be injected via the handshake of a TLS-SRP connection. This can be used to inject known credentials into the database that can be utilized to successfully complete the handshake and use the protected service. This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	9.8	More Details
CVE-2026-22207	OpenViking through version 0.1.18, prior to commit 0251c70, contains a broken access control vulnerability that allows unauthenticated attackers to gain ROOT privileges when the root_api_key configuration is omitted. Attackers can send requests to protected endpoints without authentication headers to access administrative functions including account management, resource operations, and system configuration.	9.8	More Details
CVE-2026-28213	EverShop is a TypeScript-first eCommerce platform. Versions prior to 2.1.1 have a vulnerability in the "Forgot Password" functionality. When specifying a target email address, the API response returns the password reset token. This allows an attacker to take over the associated account. Version 2.1.1 fixes the issue.	9.8	More Details
CVE-2026-3301	A security flaw has been discovered in Totolink N300RH 6.1c.1353_B20190305. Affected by this vulnerability is the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument webWlanIdx results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-27606	Rollup is a module bundler for JavaScript. Versions prior to 2.80.0, 3.30.0, and 4.59.0 of the Rollup module bundler (specifically v4.x and present in current source) is vulnerable to an Arbitrary File Write via Path Traversal. Insecure file name sanitization in the core engine allows an attacker to control output filenames (e.g., via CLI named inputs, manual chunk aliases, or malicious plugins) and use traversal sequences (`../`) to overwrite files anywhere on the host filesystem that the build process has permissions for. This can lead to persistent Remote Code Execution (RCE) by overwriting critical system or user configuration files. Versions 2.80.0, 3.30.0, and 4.59.0 contain a patch for the issue.	9.8	More Details
CVE-2025-11251	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dayneks Software Industry and Trade Inc. E-Commerce Platform allows SQL Injection.This issue affects E-Commerce Platform: through 27022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-21660	Hardcoded Email Credentials Saved as Plaintext in Firmware (CWE-256: Plaintext Storage of a Password) vulnerability in Frick Controls Quantum HD version 10.22 and prior lead to unauthorized access, exposure of sensitive information, and potential misuse or system compromise This issue affects Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2026-21659	Unauthenticated Remote Code Execution and Information Disclosure due to Local File Inclusion (LFI) vulnerability in Johnson Controls Frick Controls Quantum HD allow an unauthenticated attacker to execute arbitrary code on the affected device, leading to full system compromise. This issue affects Frick Controls Quantum HD: Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2026-2251	Improper limitation of a pathname to a restricted directory (Path Traversal) vulnerability in Xerox FreeFlow Core allows unauthorized path traversal leading to RCE. This issue affects Xerox FreeFlow Core versions up to and including 8.0.7. Please consider upgrading to FreeFlow Core version 8.1.0 via the software available on - https://www.support.xerox.com/en-us/product/core/downloads https://www.support.xerox.com/en-us/product/core/downloads	9.8	More Details
	Unauthenticated Remote Code Execution i.e Improper Control of Generation of Code ('Code		

CVE-2026-21658	Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows Code Injection. Insufficient validation of input in certain parameters may permit unexpected actions, which could impact the security of the device before authentication occurs.This issue affects Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2026-21657	Improper Control of Generation of Code ('Code Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows Code Injection. Insufficient validation of input in certain parameters may permit unexpected actions, which could impact the security of the device before authentication occurs.This issue affects Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2026-21656	Improper Control of Generation of Code ('Code Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows Code Injection. Insufficient validation of input in certain parameters may permit unexpected actions, which could impact the security of the device before authentication occurs.This issue affects Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2026-21654	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows OS Command Injection. Insufficient validation of input in certain parameters may permit unexpected actions, which could impact the security of the device before authentication occurs.This issue affects Frick Controls Quantum HD version 10.22 and prior.	9.8	More Details
CVE-2025-12981	The Listee theme for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.1.6. This is due to a broken validation check in the bundled listee-core plugin's user registration function that fails to properly sanitize the user_role parameter. This makes it possible for unauthenticated attackers to register as Administrator by manipulating the user_role parameter during registration.	9.8	More Details
CVE-2025-11252	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Signum Technology Promotion and Training Inc. Windesk.Fm allows SQL Injection.This issue affects windesk.Fm: through 27022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-27637	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.206, FreeScout's `TokenAuth` middleware uses a predictable authentication token computed as `MD5(user_id + created_at + APP_KEY)`. This token is static (never expires/rotates), and if an attacker obtains the `APP_KEY` — a well-documented and common exposure vector in Laravel applications — they can compute a valid token for any user, including the administrator, achieving full account takeover without any password. This vulnerability can be exploited on its own or in combination with CVE-2026-27636. Version 1.8.206 fixes both vulnerabilities.	9.8	More Details
CVE-2026-25146	OpenEMR is a free and open source electronic health records and medical practice management application. From 5.0.2 to before 8.0.0, there are (at least) two paths where the gateway_api_key secret value is rendered to the client in plaintext. These secret keys being leaked could result in arbitrary money movement or broad account takeover of payment gateway APIs. This vulnerability is fixed in 8.0.0.	9.6	More Details
CVE-2026-27510	Unitree Go2 firmware versions 1.1.7 through 1.1.11, when used with the Unitree Go2 Android application (com.unitree.doggo2), are vulnerable to remote code execution due to missing integrity protection and validation of user-created programmes. The Android application stores programs in a local SQLite database (unitree_go2.db, table dog_programme) and transmits the programme_text content, including the pyCode field, to the robot. The robot's actuator_manager.py executes the supplied Python as root without integrity verification or content validation. An attacker with local access to the Android device can tamper with the stored programme record to inject arbitrary Python that executes when the user triggers the program via a controller keybinding, and the malicious binding persists across reboots. Additionally, a malicious program shared through the application's community marketplace can result in arbitrary code execution on any robot that imports and runs it.	9.6	More Details
CVE-2025-69771	An arbitrary file upload vulnerability in the subtitle loading function of asbplayer v1.13.0 allows attackers to execute arbitrary code via uploading a crafted subtitle file.	9.6	More Details
	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An		

CVE-2026-27028	unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-27772	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-20781	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-24731	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-25851	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-27767	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-27614	Bugsink is a self-hosted error tracking tool. In versions prior to 2.0.13, an unauthenticated attacker who can submit events to a Bugsink project can store arbitrary JavaScript in an event. The payload executes only if a user explicitly views the affected Stacktrace in the web UI. When Pygments returns more lines than it was given (a known upstream quirk that triggers with Ruby heredoc-style input), `_pygmentize_lines()` in `theme/templatetags/issues.py:75-77` falls back to returning the raw input lines. `mark_safe()` at line 111-113 is then applied unconditionally - including to those unsanitized raw lines. Since DSN endpoints are public by Sentry protocol, no account is needed to inject. The payload sits in the database until an admin looks at the event. Successful exploitation requires that the attacker to be able to submit events to the project (i.e. knows the DSN or can access a client that uses it), the Bugsink ingest endpoint is reachable to the attacker, and an administrator explicitly views the crafted event in the UI. Under those conditions, the attacker can execute JavaScript in the administrator’s browser and act with that user’s privileges within Bugsink. Version 2.0.13 fixes the vulnerability.	9.3	More Details
CVE-2026-26266	AliasVault is a privacy-first password manager with built-in email aliasing. A stored cross-site scripting (XSS) vulnerability was identified in the email rendering feature of AliasVault Web Client versions 0.25.3 and lower. When viewing received emails on an alias, the HTML content is rendered in an iframe using srcdoc, which does not provide origin isolation. An attacker can send a crafted email containing malicious JavaScript to any AliasVault email alias. When the	9.3	More Details

	victim views the email in the web client, the script executes in the same origin as the application. No sanitization or sandboxing was applied to email HTML content before rendering. This vulnerability is fixed in 0.26.0.[		
CVE-2026-27699	The `basic-ftp` FTP client library for Node.js contains a path traversal vulnerability (CWE-22) in versions prior to 5.2.0 in the `downloadToDir()` method. A malicious FTP server can send directory listings with filenames containing path traversal sequences (`../`) that cause files to be written outside the intended download directory. Version 5.2.0 patches the issue.	9.1	More Details
CVE-2026-26279	Froxlor is open source server administration software. Prior to 2.3.4, a typo in Froxlor's input validation code (== instead of =) completely disables email format checking for all settings fields declared as email type. This allows an authenticated admin to store arbitrary strings in the panel.adminmail setting. This value is later concatenated into a shell command executed as root by a cron job, where the pipe character | is explicitly whitelisted. The result is full root-level Remote Code Execution. This vulnerability is fixed in 2.3.4.	9.1	More Details
CVE-2025-48609	In multiple functions of MmsProvider.java, there is a possible way to arbitrarily delete files which affect telephony, SMS, and MMS functionalities due to a path traversal error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	9.1	More Details
CVE-2025-1242	The administrative credentials can be extracted through application API responses, mobile application reverse engineering, and device firmware reverse engineering. The exposure may result in an attacker gaining full administrative access to the Gardyn IoT Hub exposing connected devices to malicious control.	9.1	More Details
CVE-2026-0704	In affected version of Octopus Deploy it was possible to remove files and/or contents of files on the host using an API endpoint. The field lacked validation which could potentially result in ways to circumvent expected workflows.	9.1	More Details
CVE-2026-27575	Vikunja is an open-source self-hosted task management platform. Prior to version 2.0.0, the application allows users to set weak passwords (e.g., 1234, password) without enforcing minimum strength requirements. Additionally, active sessions remain valid after a user changes their password. An attacker who compromises an account (via brute-force or credential stuffing) can maintain persistent access even after the victim resets their password. Version 2.0.0 contains a fix.	9.1	More Details
CVE-2026-27809	psd-tools is a Python package for working with Adobe Photoshop PSD files. Prior to version 1.12.2, when a PSD file contains malformed RLE-compressed image data (e.g. a literal run that extends past the expected row size), decode_rle() raises ValueError which propagated all the way to the user, crashing psd.composite() and psd-tools export. decompress() already had a fallback that replaces failed channels with black pixels when result is None, but it never triggered because the ValueError from decode_rle() was not caught. The fix in version 1.12.2 wraps the decode_rle() call in a try/except so the existing fallback handles the error gracefully.	9.1	More Details
CVE-2026-28370	In the query parser in OpenStack Vitrage before 12.0.1, 13.0.0, 14.0.0, and 15.0.0, a user allowed to access the Vitrage API may trigger code execution on the Vitrage service host as the user the Vitrage service runs under. This may result in unauthorized access to the host and further compromise of the Vitrage service. All deployments exposing the Vitrage API are affected. This occurs in _create_query_function in vitrage/graph/query.py.	9.1	More Details
CVE-2026-2750	Improper Input Validation vulnerability in Centreon Centreon Open Tickets on Central Server on Linux (Centreon Open Tickets modules).This issue affects Centreon Open Tickets on Central Server: from all before 25.10; 24.10;24.04.	9.1	More Details
CVE-2026-28215	hoppscotch is an open source API development ecosystem. Prior to version 2026.2.0, an unauthenticated attacker can overwrite the entire infrastructure configuration of a self-hosted Hoppscotch instance including OAuth provider credentials and SMTP settings by sending a single HTTP POST request with no authentication. The endpoint POST /v1/onboarding/config has no authentication guard and performs no check on whether onboarding was already completed. A successful exploit allows the attacker to replace the instance's Google/GitHub/Microsoft OAuth application credentials with their own, causing all subsequent user logins via SSO to authenticate against the attacker's OAuth app. The attacker captures OAuth tokens and email addresses of every user who logs in after the exploit. Additionally, the endpoint returns a recovery token that can be used to read all stored secrets in plaintext, including SMTP passwords and any other configured credentials. Version 2026.2.0 fixes the	9.1	More Details

	issue.		
CVE-2025-50199	Chamilo is a learning management system. Prior to version 1.11.30, there is a blind SSRF vulnerability in /index.php via the POST openid_url parameter. This issue has been patched in version 1.11.30.	9.1	More Details
CVE-2026-27822	RustFS is a distributed object storage system built in Rust. Prior to version 1.0.0-alpha.83, a Stored Cross-Site Scripting (XSS) vulnerability in the RustFS Console allows an attacker to execute arbitrary JavaScript in the context of the management console. By bypassing the PDF preview logic, an attacker can steal administrator credentials from `localStorage`, leading to full account takeover and system compromise. Version 1.0.0-alpha.83 fixes the issue.	9.0	More Details
CVE-2026-24663	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an unauthenticated attacker to achieve remote code execution on the system by sending a crafted request to the libraries installation route and injecting malicious input into the request body.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-50189	Chamilo is a learning management system. Prior to version 1.11.30, the application performs insufficient validation of data coming from the user from the POST resource[document] [SQL_INJECTION_HERE] and POST login parameters found in /main/coursecopy/copy_course_session_selected.php, which allows an attacker to perform an attack aimed at modifying the database query logic by injecting an arbitrary SQL statements. This issue has been patched in version 1.11.30.	8.8	More Details
CVE-2026-3380	A vulnerability was found in Tenda F453 1.0.0.3. This issue affects the function frmL7ImForm of the file /goform/L7Im. The manipulation of the argument page results in buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-25746	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0 contain a SQL injection vulnerability in prescription that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the prescription listing functionality. Version 8.0.0 fixes the vulnerability.	8.8	More Details
CVE-2026-3378	A flaw has been found in Tenda F453 1.0.0.3. This affects the function fromqossetting of the file /goform/qossetting. Executing a manipulation of the argument qos can lead to buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-3377	A vulnerability was detected in Tenda F453 1.0.0.3. Affected by this issue is the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. Performing a manipulation of the argument page results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-27636	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.206, FreeScout's file upload restriction list in `app/Misc/Helper.php` does not include `.htaccess` or `.user.ini` files. On Apache servers with `AllowOverride All` (a common configuration), an authenticated user can upload a `.htaccess` file to redefine how files are processed, enabling Remote Code Execution. This vulnerability can be exploited on its own or in combination with CVE-2026-27637. Version 1.8.206 fixes both vulnerabilities.	8.8	More Details
CVE-2026-27745	The SPIP interface_traduction_objets plugin versions prior to 2.2.2 contain an authenticated remote code execution vulnerability in the translation interface workflow. The plugin incorporates untrusted request data into a hidden form field that is rendered without SPIP output filtering. Because fields prefixed with an underscore bypass protection mechanisms and the hidden content is rendered with filtering disabled, an authenticated attacker with editor-level privileges can inject crafted content that is evaluated through SPIP's template processing chain, resulting in execution of code in the context of the web server.	8.8	More Details
CVE-	Zed, a code editor, has an extension installer allows tar/gzip downloads. Prior to version 0.224.4, the tar extractor (`async_tar::Archive::unpack`) creates symlinks from the archive without validation, and the path guard (`writeable_path_from_extension`) only performs lexical prefix		More

2026-27976	checks without resolving symlinks. An attacker can ship a tar that first creates a symlink inside the extension workdir pointing outside (e.g., `escape -> /`), then writes files through the symlink, causing writes to arbitrary host paths. This escapes the extension sandbox and enables code execution. Version 0.224.4 patches the issue.	8.8	Details
CVE-2026-27747	The SPIP interface_traduction_objets plugin versions prior to 2.2.2 contain an authenticated SQL injection vulnerability in interface_traduction_objets_pipelines.php. When handling translation requests, the plugin reads the id_parent parameter from user-supplied input and concatenates it directly into a SQL WHERE clause in a call to sql_getfetsel() without input validation or parameterization. An authenticated attacker with editor-level privileges can inject crafted SQL expressions into the id_parent parameter to manipulate the backend query. Successful exploitation can result in disclosure or modification of database contents and may lead to denial of service depending on the database configuration and privileges.	8.8	More Details
CVE-2026-27939	Statmatic is a Laravel and Git powered content management system (CMS). Starting in version 6.0.0 and prior to version 6.4.0, Authenticated Control Panel users may under certain conditions obtain elevated privileges without completing the intended verification step. This can allow access to sensitive operations and, depending on the user's existing permissions, may lead to privilege escalation. This has been fixed in 6.4.0.	8.8	More Details
CVE-2026-26955	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, a malicious RDP server can trigger a heap buffer overflow in FreeRDP clients using the GDI surface pipeline (e.g., `xfreerdp`) by sending an RDPGFX ClearCodec surface command with an out-of-bounds destination rectangle. The `gdi_SurfaceCommand_ClearCodec()` handler does not call `is_within_surface()` to validate the command rectangle against the destination surface dimensions, allowing attacker-controlled `cmd->left`/`cmd->top` (and subcodec rectangle offsets) to reach image copy routines that write into `surface->data` without bounds enforcement. The OOB write corrupts an adjacent `gdiGfxSurface` struct's `codecs*` pointer with attacker-controlled pixel data, and corruption of `codecs*` is sufficient to reach an indirect function pointer call (`NSC_CONTEXT.decode` at `nsc.c:500`) on a subsequent codec command — full instruction pointer (RIP) control demonstrated in exploitability harness. Users should upgrade to version 3.23.0 to receive a patch.	8.8	More Details
CVE-2026-3273	A vulnerability was identified in Tenda F453 1.0.0.3. Affected by this vulnerability is the function formWrlsafeset of the file /goform/AdvSetWrlsafeset of the component httpd. Such manipulation of the argument mit_ssid_index leads to buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-28399	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, an authenticated user with Creator role can inject arbitrary SQL via the DATEADD formula's unit parameter. This issue has been patched in version 0.301.3.	8.8	More Details
CVE-2026-3274	A security flaw has been discovered in Tenda F453 1.0.0.3. Affected by this issue is the function frmL7ProtForm of the file /goform/L7Prot of the component httpd. Performing a manipulation of the argument page results in buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-3132	The Master Addons for Elementor Premium plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.1.3 via the 'JLTMA_Widget_Admin::render_preview'. This is due to missing capability check. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute code on the server.	8.8	More Details
CVE-2026-26965	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, in the RLE planar decode path, `planar_decompress_plane_rle()` writes into `pDstData` at `((nYDst+y) * nDstStep) + (4*nXDst) + nChannel` without verifying that `(nYDst+nSrcHeight)` fits in the destination height or that `(nXDst+nSrcWidth)` fits in the destination stride. When `TempFormat != DstFormat`, `pDstData` becomes `planar->pTempData` (sized for the desktop), while `nYDst` is only validated against the **surface** by `is_within_surface()`. A malicious RDP server can exploit this to perform a heap out-of-bounds write with attacker-controlled offset and pixel data on any connecting FreeRDP client. The OOB write reaches up to 132,096 bytes past the temp buffer end, and on the brk heap (desktop ≤ 128×128), an adjacent `NSC_CONTEXT` struct's `decode` function pointer is overwritten with attacker-controlled pixel data — control-flow–relevant corruption (function pointer overwritten) demonstrated under deterministic heap layout (`nsc->decode = 0xFF414141FF414141`). Version 3.23.0 fixes the vulnerability.	8.8	More Details

CVE-2026-26186	Fleet is open source device management software. A SQL injection vulnerability in versions prior to 4.80.1 allowed authenticated users to inject arbitrary SQL expressions via the `order_key` query parameter. Due to unsafe use of `goqu.I()` when constructing the `ORDER BY` clause, specially crafted input could escape identifier quoting and be interpreted as executable SQL. An authenticated attacker with access to the affected endpoint could inject SQL expressions into the underlying MySQL query. Although the injection occurs in an `ORDER BY` context, it is sufficient to enable blind SQL injection techniques that can disclose database information through conditional expressions that affect result ordering. Crafted expressions may also cause excessive computation or query failures, potentially leading to degraded performance or denial of service. No direct evidence of reliable data modification or stacked query execution was demonstrated. Version 4.80.1 fixes the issue. If an immediate upgrade is not possible, users should restrict access to the affected endpoint to trusted roles only and ensure that any user-supplied sort or column parameters are strictly allow-listed at the application or proxy layer.	8.8	More Details
CVE-2024-31328	In broadcastIntentLockedTraced of BroadcastController.java, there is a possible way to launch arbitrary activities from the background on the paired companion phone due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2026-3165	A vulnerability was determined in Tenda F453 1.0.0.3. Impacted is the function fromSetWifiGusetBasic of the file /goform/AdvSetWrlsafeset of the component httpd. This manipulation of the argument mit_ssid causes buffer overflow. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-3275	A weakness has been identified in Tenda F453 1.0.0.3. This affects the function fromAddressNat of the file /goform/addressNat of the component httpd. Executing a manipulation of the argument entrys can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-3166	A vulnerability was identified in Tenda F453 1.0.0.3. The affected element is the function fromRouteStatic of the file /goform/RouteStatic of the component httpd. Such manipulation of the argument page leads to buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-3167	A security flaw has been discovered in Tenda F453 1.0.0.3. The impacted element is the function formWebTypeLibrary of the file /goform/webtypelibrary of the component httpd. Performing a manipulation of the argument webSiteId results in buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-3168	A weakness has been identified in Tenda F453 1.0.0.3. This affects the function fromNatStaticSetting of the file /goform/NatStaticSetting 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 made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-20430	In wlan AP FW, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00467553; Issue ID: MSV-5151.	8.8	More Details
CVE-2026-3169	A security vulnerability has been detected in Tenda F453 1.0.0.3. This impacts the function fromSafeEmailFilter of the file /goform/SafeEmailFilter of the component httpd. The manipulation of the argument page leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-28193	In JetBrains YouTrack before 2025.3.121962 apps were able to send requests to the app permissions endpoint	8.8	More Details
CVE-2026-1929	The Advanced Woo Labels plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.37. This is due to the use of `call_user_func_array()` with user-controlled callback and parameters in the `get_select_option_values()` AJAX handler without an allowlist of permitted callbacks or a capability check. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute arbitrary PHP functions and operating system commands on the server via the 'callback' parameter.	8.8	More Details
CVE-	A vulnerability has been found in Tenda F453 1.0.0.3. This vulnerability affects the function fromSetIpBind of the file /goform/SetIpBind. The manipulation of the argument page leads to		More

2026-3379	buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	Details
CVE-2026-3376	A security vulnerability has been detected in Tenda F453 1.0.0.3. Affected by this vulnerability is the function fromSafeMacFilter of the file /goform/SafeMacFilter. Such manipulation of the argument page leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-27899	WireGuard Portal (or wg-portal) is a web-based configuration portal for WireGuard server management. Prior to version 2.1.3, any authenticated non-admin user can become a full administrator by sending a single PUT request to their own user profile endpoint with `"IsAdmin": true` in the JSON body. After logging out and back in, the session picks up admin privileges from the database. When a user updates their own profile, the server parses the full JSON body into the user model, including the `IsAdmin` boolean field. A function responsible for preserving calculated or protected attributes pins certain fields to their database values (such as base model data, linked peer count, and authentication data), but it does not do this for `IsAdmin`. As a result, whatever value the client sends for `IsAdmin` is written directly to the database. After the exploit, the attacker has full admin access to the WireGuard VPN management portal. The problem was fixed in v2.1.3. The docker images for the tag 'latest' built from the master branch also include the fix.	8.8	More Details
CVE-2026-1311	The Worry Proof Backup plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 0.2.4 via the backup upload functionality. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload a malicious ZIP archive with path traversal sequences to write arbitrary files anywhere on the server, including executable PHP files. This can lead to remote code execution.	8.8	More Details
CVE-2024-55024	An authentication bypass vulnerability in the authorization mechanism of Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 allows unauthorized attackers to perform Administrative actions using service accounts.	8.8	More Details
CVE-2025-52468	Chamilo is a learning management system. Prior to version 1.11.30, an input validation vulnerability exists when importing user data from CSV files. This flaw occurs due to insufficient sanitization of user data, specifically in the "Last Name", "First Name", and "Username" fields. It allows attackers to inject a stored cross-site scripting (XSS) payload that is triggered when the user profile is viewed, potentially leading to malicious script execution in the context of the authenticated use. This issue has been patched in version 1.11.30.	8.8	More Details
CVE-2026-21853	AFFiNE is an open-source, all-in-one workspace and an operating system. Prior to version 0.25.4, there is a one-click remote code execution vulnerability. This vulnerability can be exploited by embedding a specially crafted affine: URL on a website. An attacker can trigger the vulnerability in two common scenarios: 1/ A victim visits a malicious website controlled by the attacker and the website redirect to the URL automatically, or 2/ A victim clicks on a crafted link embedded on a legitimate website (e.g., in user-generated content). In both cases, the browser invokes AFFiNE custom URL handler, which launches the AFFiNE app and processes the crafted URL. This results in arbitrary code execution on the victim’s machine, without further interaction. This issue has been patched in version 0.25.4.	8.8	More Details
CVE-2026-23627	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, an SQL injection vulnerability in the Immunization module allows any authenticated user to execute arbitrary SQL queries, leading to complete database compromise, PHI exfiltration, credential theft, and potential remote code execution. The vulnerability exists because user-supplied `patient_id` values are directly concatenated into SQL WHERE clauses without parameterization or escaping. Version 8.0.0 patches the issue.	8.8	More Details
CVE-2026-25131	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, a Broken Access Control vulnerability exists in the OpenEMR order types management system, allowing low-privilege users (such as Receptionist) to add and modify procedure types without proper authorization. This vulnerability is present in the /openemr/interface/orders/types_edit.php endpoint. Version 8.0.0 contains a patch.	8.8	More Details
CVE-2026-20126	A vulnerability in Cisco Catalyst SD-WAN Manager could allow an authenticated, local attacker with low privileges to gain root privileges on the underlying operating system. This vulnerability is due to an insufficient user authentication mechanism in the REST API. An attacker could exploit this vulnerability by sending a request to the REST API of the affected system. A successful exploit could allow the attacker to gain root privileges on the underlying operating system.	8.8	More Details

CVE-2025-12345	A security vulnerability has been detected in LLM-Claw 0.1.0/0.1.1/0.1.1a/0.1.1a-p1. The affected element is the function agent_deploy_init of the file /agents/deploy/initiate.c of the component Agent Deployment. Such manipulation leads to buffer overflow. It is possible to launch the attack remotely. A patch should be applied to remediate this issue.	8.8	More Details
CVE-2026-2448	The Page Builder by SiteOrigin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.33.5 via the locate_template() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2026-1565	The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'WPUF_Admin_Settings::check_filetype_and_ext' function and in the 'Admin_Tools::check_filetype_and_ext' function in all versions up to, and including, 4.2.8. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2026-24502	Dell Command | Intel vPro Out of Band, versions prior to 4.7.0, contain an Uncontrolled Search Path Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	8.8	More Details
CVE-2026-26699	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to arbitrary code execution in ip/ppes/admin/admin_change_picture.php.	8.8	More Details
CVE-2026-27969	Vitess is a database clustering system for horizontal scaling of MySQL. Prior to versions 23.0.3 and 22.0.4, anyone with read/write access to the backup storage location (e.g. an S3 bucket) can manipulate backup manifest files so that files in the manifest — which may be files that they have also added to the manifest and backup contents — are written to any accessible location on restore. This is a common path traversal security issue. This can be used to provide that attacker with unintended/unauthorized access to the production deployment environment — allowing them to access information available in that environment as well as run any additional arbitrary commands there. Versions 23.0.3 and 22.0.4 contain a patch. No known workarounds are available.	8.8	More Details
CVE-2026-3399	A vulnerability was identified in Tenda F453 1.0.0.3. Affected by this vulnerability is the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer of the component httpd. The manipulation of the argument dips leads to buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-27961	Agenta is an open-source LLMOps platform. A Server-Side Template Injection (SSTI) vulnerability exists in versions prior to 0.86.8 in Agenta's API server evaluator template rendering. Although the vulnerable code lives in the SDK package, it is executed server-side within the API process when running evaluators. This does not affect standalone SDK usage — it only impacts self-hosted or managed Agenta platform deployments. Version 0.86.8 contains a fix for the issue.	8.8	More Details
CVE-2026-1566	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 5.2.7. This is due to the plugin allowing users with a LatePoint Agent role, who are creating new customers to set the 'wordpress_user_id' field. This makes it possible for authenticated attackers, with Agent-level access and above, to gain elevated privileges by linking a customer to the arbitrary user ID, including administrators, and then resetting the password.	8.8	More Details
CVE-2026-27952	Agenta is an open-source LLMOps platform. In Agenta-API prior to version 0.48.1, a Python sandbox escape vulnerability existed in Agenta's custom code evaluator. Agenta used RestrictedPython as a sandboxing mechanism for user-supplied evaluator code, but incorrectly whitelisted the `numpy` package as safe within the sandbox. This allowed authenticated users to bypass the sandbox and achieve arbitrary code execution on the API server. The escape path was through `numpy.ma.core.inspect`, which exposes Python's introspection utilities — including `sys.modules` — thereby providing access to unfiltered system-level functionality like `os.system`. This vulnerability affects the Agenta self-hosted platform (API server), not the SDK when used as a standalone Python library. The custom code evaluator runs server-side within the API process. The issue is fixed in v0.48.1 by removing `numpy` from the sandbox allowlist. In later	8.8	More Details

	versions (v0.60+), the RestrictedPython sandbox was removed entirely and replaced with a different execution model.		
CVE-2026-3400	A security flaw has been discovered in Tenda AC15 up to 15.13.07.13. Affected by this issue is some unknown functionality of the file /goform/TextEditingConversion. The manipulation of the argument wpapsk_crypto2_4g results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-3271	A vulnerability was found in Tenda F453 1.0.0.3. This impacts the function fromP2pListFilter of the file /goform/P2pListFilterof of the component httpd. The manipulation of the argument page results in buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-3398	A vulnerability was determined in Tenda F453 1.0.0.3. Affected is the function fromAdvSetWan of the file /goform/AdvSetWan of the component httpd. Executing a manipulation of the argument wanmode/PPPOEPassword can lead to buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-3272	A vulnerability was determined in Tenda F453 1.0.0.3. Affected is the function fromDhcpListClient of the file /goform/DhcpListClient of the component httpd. This manipulation of the argument page causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-22206	SPIP versions prior to 4.4.10 contain a SQL injection vulnerability that allows authenticated low-privilege users to execute arbitrary SQL queries by manipulating union-based injection techniques. Attackers can exploit this SQL injection flaw combined with PHP tag processing to achieve remote code execution on the server.	8.8	More Details
CVE-2025-69437	PublicCMS v5.202506.d and earlier is vulnerable to stored XSS. Uploaded PDFs can contain JavaScript payloads and bypass PDF security checks in the backend CmsFileUtils.java. If a user uploads a PDF file containing a malicious payload to the system and views it, the embedded JavaScript payload can be triggered, resulting in issues such as credential theft, arbitrary API execution, and other security concerns. This vulnerability affects all file upload endpoint, including /cmsTemplate/save, /file/doUpload, /cmsTemplate/doUpload, /file/doBatchUpload, /cmsWebFile/doUpload, etc.	8.7	More Details
CVE-2025-69231	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, a stored cross-site scripting vulnerability in the GAD-7 anxiety assessment form allows authenticated users with clinician privileges to inject malicious JavaScript that executes when other users view the form. This enables session hijacking, account takeover, and privilege escalation from clinician to administrator. Version 8.0.0 fixes the issue.	8.7	More Details
CVE-2026-28274	Initiative is a self-hosted project management platform. Versions of the application prior to 0.32.4 are vulnerable to Stored Cross-Site Scripting (XSS) in the document upload functionality. Any user with upload permissions within the "Initiatives" section can upload a malicious `.html` or `.htm` file as a document. Because the uploaded HTML file is served under the application's origin without proper sandboxing, the embedded JavaScript executes in the context of the application. As a result, authentication tokens, session cookies, or other sensitive data can be exfiltrated to an attacker-controlled server. Additionally, since the uploaded file is hosted under the application's domain, simply sharing the direct file link may result in execution of the malicious script when accessed. Version 0.32.4 fixes the issue.	8.7	More Details
CVE-2026-28426	Statmatic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.11 and 6.4.0, stored XSS vulnerability in svg and icon related components allow authenticated users with appropriate permissions to inject malicious JavaScript that executes when viewed by higher-privileged users. This has been fixed in 5.73.11 and 6.4.0.	8.7	More Details
CVE-2026-0007	In writeToParcel of WindowInfo.cpp, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.6	More Details
CVE-2026-27696	changedetection.io is a free open source web page change detection tool. In versions prior to 0.54.1, changedetection.io is vulnerable to Server-Side Request Forgery (SSRF) because the URL validation function `is_safe_valid_url()` does not validate the resolved IP address of watch URLs against private, loopback, or link-local address ranges. An authenticated user (or any user when no password is configured, which is the default) can add a watch for internal network URLs. The application fetches these URLs server-side, stores the response content, and makes it viewable	8.6	More Details

	through the web UI — enabling full data exfiltration from internal services. Version 0.54.1 contains a fix for the issue.		
CVE-2026-26938	Improper Neutralization of Special Elements Used in a Template Engine (CWE-1336) exists in Workflows in Kibana which could allow an attacker to read arbitrary files from the Kibana server filesystem, and perform Server-Side Request Forgery (SSRF) via Code Injection (CAPEC-242). This requires an authenticated user who has the workflowsManagement:executeWorkflow privilege.	8.6	More Details
CVE-2026-25085	A vulnerability exists in Copeland XWEB Pro version 1.12.1 and prior, in which an unexpected return value from the authentication routine is later on processed as a legitimate value, resulting in an authentication bypass.	8.6	More Details
CVE-2026-28286	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.5.2-beta3, the application enforces restrictions in the frontend/UI to prevent users from creating files or folders in internal OS paths. However, when interacting directly with the API, the restrictions are bypass-able. By sending a crafted request targeting paths like /etc, /usr, or other sensitive system directories, the API successfully creates files or directories in locations where normal users should have no write access. This indicates that the API does not properly validate the target path, allowing unauthorized operations on critical system directories. No known patch is publicly available.	8.5	More Details
CVE-2025-48579	In multiple functions of MediaProvider.java, there is a possible external storage write permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48574	In validateAddingWindowLw of DisplayPolicy.java, there is a possible way for an app to intercept drag-and-drop events due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-32313	In UsageEvents of UsageEvents.java, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48636	In openFile of BugreportContentProvider.java, there is a possible way to read and write unauthorized files due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48582	In multiple locations, there is a possible way to delete media without the MANAGE_EXTERNAL_STORAGE permission due to an intent redirect. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48602	In exitKeyguardAndFinishSurfaceBehindRemoteAnimation of KeyguardViewMediator.java, there is a possible lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48605	In multiple functions of KeyguardViewMediator.java, there is a possible lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-48619	In multiple functions of ContentProvider.java, there is a possible way for an app with read-only access to truncate files due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-3071	Deserialization of untrusted data in the LanguageModel class of Flair from versions 0.4.1 to latest are vulnerable to arbitrary code execution when loading a malicious model.	8.4	More Details
CVE-2026-0037	In multiple functions of ffa.c, there is a possible memory corruption due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-	In hasImage of Notification.java, there is a possible way to reveal information across users due to a permissions bypass. This could lead to local escalation of privilege with no additional execution	8.4	More Details

0025	privileges needed. User interaction is not needed for exploitation.		
CVE-2026-0020	In parsePermissionGroup of ParsedPermissionUtils.java, there is a possible way to bypass a consent dialog to obtain permissions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0013	In setupLayout of PickActivity.java, there is a possible way to start any activity as a DocumentsUI app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0011	In enableSystemPackageLPw of Settings.java, there is a possible way to prevent location access from working due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0035	In createRequest of MediaProvider.java, there is a possible way for an app to gain read/write access to non-existing files due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0031	In multiple functions of mem_protect.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0010	In onTransact of IDrmManagerService.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0038	In multiple functions of mem_protect.c, there is a possible way to execute arbitrary code due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0047	In dumpBitmapsProto of ActivityManagerService.java, there is a possible way for an app to access private information due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0008	In multiple locations, there is a possible privilege escalation due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0028	In __pkvm_host_share_guest of mem_protect.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-21882	theshit is a command-line utility that automatically detects and fixes common mistakes in shell commands. Prior to version 0.2.0, improper privilege dropping allows local privilege escalation via command re-execution. This issue has been patched in version 0.2.0.	8.4	More Details
CVE-2025-48650	In multiple locations, there is a possible information disclosure due to SQL injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0029	In __pkvm_init_vm of pkvm.c, there is a possible memory corruption due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0034	In setPackageOrComponentEnabled of ManagedServices.java, there is a possible notification policy desync due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0030	In __host_check_page_state_range of mem_protect.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-0021	In hasInteractAcrossUsersFullPermission of AppInfoBase.java, there is a possible cross-user permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details

CVE-2026-26861	CleverTap Web SDK version 1.15.2 and earlier is vulnerable to Cross-Site Scripting (XSS) via window.postMessage. The handleCustomHtmlPreviewPostMessageEvent function in src/util/campaignRender/nativeDisplay.js performs insufficient origin validation using the includes() method, which can be bypassed by an attacker using a subdomain	8.3	More Details
CVE-2026-26862	CleverTap Web SDK version 1.15.2 and earlier is vulnerable to DOM-based Cross-Site Scripting (XSS) via window.postMessage in the Visual Builder module. The origin validation in src/modules/visualBuilder/pageBuilder.js (lines 56-60) uses the includes() method to verify the originUrl contains "dashboard.clevertap.com", which can be bypassed by an attacker using a crafted subdomain	8.3	More Details
CVE-2026-0980	A flaw was found in rubyipmi, a gem used in the Baseboard Management Controller (BMC) component of Red Hat Satellite. An authenticated attacker with host creation or update permissions could exploit this vulnerability by crafting a malicious username for the BMC interface. This could lead to remote code execution (RCE) on the system.	8.3	More Details
CVE-2026-2751	Blind SQL Injection via unsanitized array keys in Service Dependencies deletion. Vulnerability in Centreon Centreon Web on Central Server on Linux (Service Dependencies modules) allows Blind SQL Injection.This issue affects Centreon Web on Central Server before 25.10.8, 24.10.20, 24.04.24.	8.3	More Details
CVE-2026-28216	hoppscotch is an open source API development ecosystem. Prior to version 2026.2.0, any logged-in user can read, modify or delete another user's personal environment by ID. `user-environments.resolver.ts:82-109`, `updateUserEnvironment` mutation uses `@UseGuards(GqlAuthGuard)` but is missing the `@GqlUser()` decorator entirely. The user's identity is never extracted, so the service receives only the environment ID and performs a `prisma.userEnvironment.update({ where: { id } })` without any ownership filter. `deleteUserEnvironment` does extract the user but the service only uses the UID to check if the target is a global environment. Actual delete query uses WHERE { id } without AND userUid. hoppscotch environments store API keys, auth tokens and secrets used in API requests. An authenticated attacker who obtains another user's environment ID can read their secrets, replace them with malicious values or delete them entirely. The environment ID format is CUID, which limits mass exploitation but insider threat and combined info leak scenarios are realistic. Version 2026.2.0 fixes the issue.	8.3	More Details
CVE-2025-52482	Chamilo is a learning management system. Prior to version 1.11.30, a Stored XSS vulnerability exists in the glossary function, enabling all users with the Teachers role to inject JavaScript malicious code against the administrator. This issue has been patched in version 1.11.30.	8.3	More Details
CVE-2025-67601	A vulnerability has been identified within Rancher Manager, where using self-signed CA certificates and passing the -skip-verify flag to the Rancher CLI login command without also passing the –cacert flag results in the CLI attempting to fetch CA certificates stored in Rancher’s setting cacerts.	8.3	More Details
CVE-2025-40932	Apache::SessionX versions through 2.01 for Perl create insecure session id. Apache::SessionX generates session ids insecurely. The default session id generator in Apache::SessionX::Generate::MD5 returns a MD5 hash seeded with the built-in rand() function, the epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems.	8.2	More Details
CVE-2026-27627	Karakeep is a elf-hostable bookmark-everything app. In version 0.30.0, when the Reddit metascraper plugin returns `readableContentHtml`, the HTML parsing subprocess uses it directly without running it through DOMPurify. Every other content source in the crawler goes through Readability + DOMPurify, but the Reddit path skips both. Since this content ends up in `dangerouslySetInnerHTML` in the reader view, any malicious HTML in the Reddit response gets executed in the user's browser. Version 0.31.0 contains a patch for this issue.	8.2	More Details
CVE-2025-71057	Improper session management in D-Link Wireless N 300 ADSL2+ Modem Router DSL-124 ME_1.00 allows attackers to execute a session hijacking attack via spoofing the IP address of an authenticated user.	8.2	More Details
CVE-2026-28562	wpForo 2.4.14 contains an unauthenticated SQL injection vulnerability in Topics::get_topics() where the ORDER BY clause relies on ineffective esc_sql() sanitization on unquoted identifiers. Attackers exploit the wpfob parameter with CASE WHEN payloads to perform blind boolean	8.2	More Details

	extraction of credentials from the WordPress database.		
CVE-2019-25492	Homey BNB V4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'pt' parameter. Attackers can send GET requests to the admin/getcmsdata.php endpoint with malicious 'pt' values to extract sensitive database information.	8.2	More Details
CVE-2026-28416	Gradio is an open-source Python package designed for quick prototyping. Prior to version 6.6.0, a Server-Side Request Forgery (SSRF) vulnerability in Gradio allows an attacker to make arbitrary HTTP requests from a victim's server by hosting a malicious Gradio Space. When a victim application uses `gr.load()` to load an attacker-controlled Space, the malicious `proxy_url` from the config is trusted and added to the allowlist, enabling the attacker to access internal services, cloud metadata endpoints, and private networks through the victim's infrastructure. Version 6.6.0 fixes the issue.	8.2	More Details
CVE-2026-28406	kaniko is a tool to build container images from a Dockerfile, inside a container or Kubernetes cluster. Starting in version 1.25.4 and prior to version 1.25.10, kaniko unpacks build context archives using `filepath.Join(dest, cleanedName)` without enforcing that the final path stays within `dest`. A tar entry like `../outside.txt` escapes the extraction root and writes files outside the destination directory. In environments with registry authentication, this can be chained with docker credential helpers to achieve code execution within the executor process. Version 1.25.10 uses securejoin for path resolution in tar extraction.	8.2	More Details
CVE-2026-27700	Hono is a Web application framework that provides support for any JavaScript runtime. In versions 4.12.0 and 4.12.1, when using the AWS Lambda adapter (`hono/aws-lambda`) behind an Application Load Balancer (ALB), the `getConnInfo()` function incorrectly selected the first value from the `X-Forwarded-For` header. Because AWS ALB appends the real client IP address to the end of the `X-Forwarded-For` header, the first value can be attacker-controlled. This could allow IP-based access control mechanisms (such as the `ipRestriction` middleware) to be bypassed. Version 4.12.2 patches the issue.	8.2	More Details
CVE-2019-25493	Homey BNB V4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'val' parameter. Attackers can send GET requests to the admin/getrecord.php endpoint with malicious 'val' values to extract sensitive database information.	8.2	More Details
CVE-2019-25497	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the currency parameter. Attackers can send GET requests to shopping_cart.php with malicious currency values using boolean-based SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2019-25496	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the products_id parameter. Attackers can modify the products_id value in product_info.php requests and append boolean-based SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2019-25491	Homey BNB V4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the catid parameter. Attackers can send GET requests to the admin/cms_getpagetitle.php endpoint with malicious catid values to extract sensitive database information.	8.2	More Details
CVE-2019-25495	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the reviews_id parameter. Attackers can send GET requests to product_reviews_write.php with malicious reviews_id values using boolean-based SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2019-25489	Homey BNB V4 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the hosting_id parameter. Attackers can send GET requests to the rooms/ajax_refresh_subtotal endpoint with malicious hosting_id values to extract sensitive database information or cause denial of service.	8.2	More Details
CVE-2019-25490	Homey BNB V4 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'id' parameter. Attackers can send GET requests to the admin/edit.php endpoint with time-based SQL injection payloads to extract sensitive database information.	8.2	More Details
	Homey BNB V4 contains an SQL injection vulnerability in the administration panel login that		

CVE-2019-25494	allows unauthenticated attackers to bypass authentication by injecting SQL syntax into username and password fields. Attackers can submit SQL operators like '=' 'or' in both credentials to manipulate the authentication query and gain unauthorized access to the admin panel.	8.2	More Details
CVE-2026-28275	Initiative is a self-hosted project management platform. Versions of the application prior to 0.32.4 do not invalidate previously issued JWT access tokens after a user changes their password. As a result, older tokens remain valid until expiration and can still be used to access protected API endpoints. This behavior allows continued authenticated access even after the account password has been updated. Version 0.32.4 fixes the issue.	8.1	More Details
CVE-2026-26985	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. Starting in version 24.0.0 and prior to versions 26.0.5, 27.0.2, and 28.0.0, an authenticated user with the appropriate authorization can read configuration files on the server by exploiting a path traversal vulnerability. Some of these files contain hard-coded credentials. The vulnerability allows an attacker to read configuration files containing hard-coded credentials. The attacker could then authenticate to the database or other services if those credentials are reused. The attacker must be authenticated and have the required permissions. However, the vulnerability is easy to exploit and the application source code is public. This problem is fixed in LORIS v26.0.5 and v27.0.2 and above, and v28.0.0 and above. As a workaround, the electrophysiogy_browser in LORIS can be disabled by an administrator using the module manager.	8.1	More Details
CVE-2026-23750	Golioth Pouch version 0.1.0, prior to commit 1b2219a1, contains a heap-based buffer overflow in BLE GATT server certificate handling. server_cert_write() allocates a heap buffer of size CONFIG_POUCH_SERVER_CERT_MAX_LEN when receiving the first fragment, then appends subsequent fragments using memcpy() without verifying that sufficient capacity remains. An adjacent BLE client can send unauthenticated fragments whose combined size exceeds the allocated buffer, causing a heap overflow and crash; integrity impact is also possible due to memory corruption.	8.1	More Details
CVE-2026-24890	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, an authorization bypass vulnerability in the patient portal signature endpoint allows authenticated portal users to upload and overwrite provider signatures by setting `type=admin-signature` and specifying any provider user ID. This could potentially lead to signature forgery on medical documents, legal compliance violations, and fraud. The issue occurs when portal users are allowed to modify provider signatures without proper authorization checks. Version 8.0.0 fixes the issue.	8.1	More Details
CVE-2026-1779	The User Registration & Membership plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.1.2. This is due to incorrect authentication in the 'register_member' function. This makes it possible for unauthenticated attackers to log in a newly registered user on the site who has the 'urm_user_just_created' user meta set.	8.1	More Details
CVE-2026-25136	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. A reflected Cross-site Scripting vulnerability was located in versions prior to 35.8.3, 38.5.4, and 39.3.1 in the rendering of the ExceptionMessage of the WebUI 500 error which could allow attackers to steal login session tokens of users who navigate to a specially crafted URL. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	8.1	More Details
CVE-2026-3172	Buffer overflow in parallel HNSW index build in pgvector 0.6.0 through 0.8.1 allows a database user to leak sensitive data from other relations or crash the database server.	8.1	More Details
CVE-2026-22719	VMware Aria Operations contains a command injection vulnerability. A malicious unauthenticated actor may exploit this issue to execute arbitrary commands which may lead to remote code execution in VMware Aria Operations while support-assisted product migration is in progress. To remediate CVE-2026-22719, apply the patches listed in the 'Fixed Version' column of the ' Response Matrix https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947 ' in VMSA-2026-0001 Workarounds for CVE-2026-22719 are documented in the 'Workarounds' column of the ' Response Matrix https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947 ' in VMSA-2026-0001	8.1	More Details
CVE-2026-	Kiteworks is a private data network (PDN). Prior to version 9.2.0, a vulnerability in Kiteworks Email Protection Gateway allows authenticated administrators to inject malicious scripts through a		More

28272	configuration interface. The stored script executes when users interact with the affected user interface. Version 9.2.0 contains a patch for the issue.	8.1	Details
CVE-2026-25164	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the REST API route table in `apis/routes/_rest_routes_standard.inc.php` does not call `RestConfig::request_authorization_check()` for the document and insurance routes. Other patient routes in the same file (e.g. encounters, patients/med) call it with the appropriate ACL. As a result, any valid API bearer token can access or modify every patient's documents and insurance data, regardless of the token's OpenEMR ACLs—effectively exposing all document and insurance PHI to any authenticated API client. Version 8.0.0 patches the issue.	8.1	More Details
CVE-2026-3179	The FTP Backup on the ADM does not properly sanitize filenames received from the FTP server when parsing directory listings. A malicious server or MITM attacker can craft filenames containing path traversal sequences, causing the client to write files outside the intended backup directory. A path traversal vulnerability may allow an attacker to overwrite arbitrary files on the system and potentially achieve privilege escalation or remote code execution. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.2.RE51.	8.1	More Details
CVE-2025-67752	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 7.0.4, OpenEMR's HTTP client wrapper (`oeHttp`/`oeHttpRequest`) disables SSL/TLS certificate verification by default (`verify: false`), making all external HTTPS connections vulnerable to man-in-the-middle (MITM) attacks. This affects communication with government healthcare APIs and user-configurable external services, potentially exposing Protected Health Information (PHI). Version 7.0.4 fixes the issue.	8.1	More Details
CVE-2026-20777	A heap-based buffer overflow vulnerability exists in the Nicolet WFT parsing functionality of The Biosig Project libbiosig 3.9.2 and Master Branch (db9a9a63). A specially crafted .wft file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2026-27607	RustFS is a distributed object storage system built in Rust. In versions 1.0.0-alpha.56 through 1.0.0-alpha.82, RustFS does not validate policy conditions in presigned POST uploads (PostObject), allowing attackers to bypass content-length-range, starts-with, and Content-Type constraints. This enables unauthorized file uploads exceeding size limits, uploads to arbitrary object keys, and content-type spoofing, potentially leading to storage exhaustion, unauthorized data access, and security bypasses. Version 1.0.0-alpha.83 fixes the issue.	8.1	More Details
CVE-2026-27608	Parse Dashboard is a standalone dashboard for managing Parse Server apps. In versions 7.3.0-alpha.42 through 9.0.0-alpha.7, the AI Agent API endpoint (`POST /apps/:appId/agent`) does not enforce authorization. Authenticated users scoped to specific apps can access any other app's agent endpoint by changing the app ID in the URL. Read-only users are given the full master key instead of the read-only master key and can supply write permissions in the request body to perform write and delete operations. Only dashboards with `agent` configuration enabled are affected. The fix in version 9.0.0-alpha.8 adds per-app authorization checks and restricts read-only users to the `readOnlyMasterKey` with write permissions stripped server-side. As a workaround, remove the `agent` configuration block from your dashboard configuration. Dashboards without an `agent` config are not affected.	8.1	More Details
CVE-2026-21389	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the request body sent to the contacts import route.	8.0	More Details
CVE-2026-24517	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into requests sent to the firmware update route.	8.0	More Details
CVE-2026-25109	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the devices field when accessing the get setup route, leading to remote code execution.	8.0	More Details
CVE-2026-0752	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.2 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that under certain circumstances, could have allowed an unauthenticated user to inject arbitrary scripts into the Mermaid sandbox UI.	8.0	More Details
CVE-	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an		More

2026-20742	authenticated attacker to achieve remote code execution on the system by injecting malicious input into requests sent to the templates route.	8.0	Details
CVE-2026-20902	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the map filename field during the map upload action of the parameters route.	8.0	More Details
CVE-2026-28425	Statmatic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.11 and 6.4.0, an authenticated control panel user with access to Antlers-enabled inputs may be able to achieve remote code execution in the application context. That can lead to full compromise of the application, including access to sensitive configuration, modification or exfiltration of data, and potential impact on availability. Exploitation is only possible where Antlers runs on user-controlled content—for example, content fields with Antlers explicitly enabled (requiring permission to configure fields and to edit entries), built-in config that supports Antlers such as Forms email notification settings (requiring configuration permission), or third-party addons that add Antlers-enabled fields to entries (for example, the SEO Pro addon). In each case the attacker must have the relevant control panel permissions. This has been fixed in 5.73.11 and 6.4.0. Users of addons that depend on Statamic should ensure that after updating they are running a patched Statamic version.	8.0	More Details
CVE-2026-20910	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the devices field of the firmware update update action to achieve remote code execution.	8.0	More Details
CVE-2026-22720	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with privileges to create custom benchmarks may be able to inject script to perform administrative actions in VMware Aria Operations. To remediate CVE-2026-22720, apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' of VMSA-2026-0001 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947https:// .	8.0	More Details
CVE-2026-25195	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by supplying a crafted firmware update file via the firmware update route.	8.0	More Details
CVE-2026-20764	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by providing malicious input via the device hostname configuration which is later processed during system setup, resulting in remote code execution.	8.0	More Details
CVE-2026-25111	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into requests sent to the restore route.	8.0	More Details
CVE-2026-24689	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the devices field of the firmware update apply action.	8.0	More Details
CVE-2026-3037	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by modifying malicious input injected into the MBird SMS service URL and/or code via the utility route which is later processed during system setup, leading to remote code execution.	8.0	More Details
CVE-2026-23702	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by sending malicious input injected into the server username field of the import preconfiguration action in the API V1 route.	8.0	More Details
CVE-2026-25721	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the server username and/or password fields of the restore action in the API V1 route.	8.0	More Details
CVE-2026-25196	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into the Wi-Fi SSID and/or password fields can lead to remote code execution when the configuration is processed.	8.0	More Details

CVE-2026-24695	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into OpenSSL argument fields within requests sent to the utility route, leading to remote code execution.	8.0	More Details
CVE-2026-25105	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by injecting malicious input into parameters of the Modbus command tool in the debug route.	8.0	More Details
CVE-2026-25037	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by configuring a maliciously crafted LCD state which is later processed during system setup, enabling remote code execution.	8.0	More Details
CVE-2026-27509	Unitree Go2 firmware versions V1.1.7 through V1.1.9 and V1.1.11 (EDU) do not implement DDS authentication or authorization for the Eclipse CycloneDDS topic rt/api/programming_actuator/request handled by actuator_manager.py. A network-adjacent, unauthenticated attacker can join DDS domain 0 and publish a crafted message (api_id=1002) containing arbitrary Python, which the robot writes to disk under /unitree/etc/programming/ and binds to a physical controller keybinding. When the keybinding is pressed, the code executes as root and the binding persists across reboots.	8.0	More Details
CVE-2026-24452	An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an authenticated attacker to achieve remote code execution on the system by supplying a crafted template file to the devices route.	8.0	More Details
CVE-2026-28364	In OCaml before 4.14.3 and 5.x before 5.4.1, a buffer over-read in Marshal deserialization (runtime/intern.c) enables remote code execution through a multi-phase attack chain. The vulnerability stems from missing bounds validation in the readblock() function, which performs unbounded memcpy() operations using attacker-controlled lengths from crafted Marshal data.	7.9	More Details
CVE-2025-48646	In executeRequest of ActivityStarter.java, there is a possible launch anywhere due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2025-48567	In multiple locations, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2025-48578	In multiple functions of MediaProvider.java, there is a possible way to bypass the WRITE_EXTERNAL_STORAGE permission due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2025-48613	In VBMeta, there is a possible way to modify and resign VBMeta using a test key, assuming the original image was previously signed with the same key. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48645	In loadDescription of DeviceAdminInfo.java, there is a possible persistent package due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-0023	In createSessionInternal of PackageInstallerService.java, there is a possible way for an app to update its ownership due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-27615	ADB Explorer is a fluent UI for ADB on Windows. In versions prior to Beta 0.9.26022, ADB-Explorer allows the `ManualAdbPath` settings variable, which determines the path of the ADB binary to be executed, to be set to a Universal Naming Convention (UNC) path in the application's settings file. This allows an attacker to set the binary's path to point to a remote network resource, hosted on an attacker-controlled network share, thus granting the attacker full control over the binary being executed by the app. An attacker may leverage this vulnerability to execute code remotely on a victim's machine with the privileges of the user running the app. Exploitation is made possible by convincing a victim to run a shortcut of the app that points to a custom `App.txt` settings file,	7.8	More Details

	which sets `ManualAdbPath` (for example, when downloaded in an archive file). Version Beta 0.9.26022 fixes the issue.		
CVE-2026-20423	In wlan STA driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00465314; Issue ID: MSV-4956.	7.8	More Details
CVE-2025-48653	In loadDataAndPostValue of multiple files, there is a possible way to obscure permission usage due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48654	In onStart of CompanionDeviceManagerService.java, there is a possible confused deputy due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-1442	Since the encryption algorithm used to protect firmware updates is itself encrypted using key material available to an attacker (or anyone paying attention), the firmware updates may be altered by an unauthorized user, and then trusted by a Unitree product, such as the Unitree Go2 and other models. This issue appears to affect all of Unitree’s current offerings as of February 26, 2026, and so should be considered a vulnerability in both the firmware generation and extraction processes. At the time of this release, there is no publicly-documented mechanism to subvert the update process and insert poisoned firmware packages without the equipment owner’s knowledge.	7.8	More Details
CVE-2026-0032	In multiple functions of mem_protect.c, there is a possible out-of-bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-0026	In removePermission of PermissionManagerServiceImpl.java, there is a possible way to override any system permission due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2026-21385	Memory corruption while using alignments for memory allocation.	7.8	More Details
CVE-2026-28211	The NVDA Dev & Test Toolbox is an NVDA add-on for gathering tools to help NVDA development and testing. A vulnerability exists in versions 2.0 through 8.0 in the Log Reader feature of this add-on. A maliciously crafted log file can lead to arbitrary code execution when a user reads it with log reader commands. The log reading command process speech log entries in an unsafe manner. Python expressions embedded in the log may be evaluated when when speech entries are read with log reading commands. An attacker can exploit this by convincing a user to open a malicious crafted log file and to analyze it using the log reading commands. When the log is read, attacker-controlled code may execute with the privileges of the current user. This issue does not require elevated privileges and relies solely on user interaction (opening the log file). Version 9.0 contains a fix for the issue. As a workaround, avoid using log reading commands, or at least, commands to move to next/previous log message (any message or commands for each type of message). For more security, one may disable their gestures in the input gesture dialog.	7.8	More Details
CVE-2025-59600	Memory Corruption when adding user-supplied data without checking available buffer space.	7.8	More Details
CVE-2025-47377	Memory Corruption when accessing a buffer after it has been freed while processing IOCTL calls.	7.8	More Details
CVE-2026-28518	OpenViking versions 0.2.1 and prior, fixed in commit 46b3e76, contain a path traversal vulnerability in the .ovpack import handling that allows attackers to write files outside the intended import directory. Attackers can craft malicious ZIP archives with traversal sequences, absolute paths, or drive prefixes in member names to overwrite or create arbitrary files with the importing process privileges.	7.8	More Details
CVE-2025-47375	Memory corruption while handling different IOCTL calls from the user-space simultaneously.	7.8	More Details

CVE-2025-47379	Memory Corruption when concurrent access to shared buffer occurs due to improper synchronization between assignment and deallocation of buffer resources.	7.8	More Details
CVE-2025-47381	Memory Corruption while processing IOCTL calls when concurrent access to shared buffer occurs.	7.8	More Details
CVE-2025-47373	Memory Corruption when accessing buffers with invalid length during TA invocation.	7.8	More Details
CVE-2025-47385	Memory Corruption when accessing trusted execution environment without proper privilege check.	7.8	More Details
CVE-2025-52365	A command injection vulnerability in the szc script of the ccurtsinger/stabilizer repository allows remote attackers to execute arbitrary system commands via unsanitized user input passed to os.system(). The vulnerability arises from improper input handling where command-line arguments are directly concatenated into shell commands without validation	7.8	More Details
CVE-2025-47386	Memory Corruption while invoking IOCTL calls when concurrent access to shared buffer occurs.	7.8	More Details
CVE-2026-2914	CyberArk Endpoint Privilege Manager Agent versions 25.10.0 and lower allow potential unauthorized privilege elevation leveraging CyberArk elevation dialogs	7.8	More Details
CVE-2025-47376	Memory Corruption when concurrent access to shared buffer occurs during IOCTL calls.	7.8	More Details
CVE-2025-59603	Memory Corruption when processing invalid user address with nonstandard buffer address.	7.8	More Details
CVE-2026-26682	An issue in fastCMS before v.0.1.6 allows a local attacker to execute arbitrary code via the PluginController.java component	7.8	More Details
CVE-2025-48635	In multiple functions of TaskFragmentOrganizerController.java, there is a possible activity token leak due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.7	More Details
CVE-2026-27938	WPGraphQL provides a GraphQL API for WordPress sites. Prior to version 2.9.1, the `wp-graphql/wp-graphql` repository contains a GitHub Actions workflow (`release.yml`) vulnerable to OS command injection through direct use of `${{ github.event.pull_request.body }}` inside a `run:` shell block. When a pull request from `develop` to `master` is merged, the PR body is injected verbatim into a shell command, allowing arbitrary command execution on the Actions runner. Version 2.9.1 contains a fix for the vulnerability.	7.7	More Details
CVE-2026-20048	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper processing when parsing SNMP requests. An attacker could exploit this vulnerability by continuously sending SNMP queries to a specific MIB of an affected device. A successful exploit could allow the attacker to cause a kernel panic on the device, resulting in a reload and a DoS condition. Note: This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMPv1 or SNMPv2c, the attacker must have a valid read-only SNMP community string for the affected system. To exploit this vulnerability through SNMPv3, the attacker must have valid SNMP user credentials for the affected system.	7.7	More Details
CVE-	Plane is an an open-source project management tool. Prior to version 1.2.2, a Full Read Server-Side Request Forgery (SSRF) vulnerability has been identified in the "Add Link" feature. This flaw allows an authenticated attacker with general user privileges to send arbitrary GET requests to		More

2026-27706	the internal network and exfiltrate the full response body. By exploiting this vulnerability, an attacker can steal sensitive data from internal services and cloud metadata endpoints. Version 1.2.2 fixes the issue.	7.7	Details
CVE-2026-0017	In onChange of BiometricService.java, there is a possible way to enable fingerprint unlock due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.7	More Details
CVE-2026-28403	Textream is a free macOS teleprompter app. Prior to version 1.5.1, the `DirectorServer` WebSocket server (`ws://127.0.0.1:<httpPort+1>`) accepts connections from any origin without validating the HTTP `Origin` header during the WebSocket handshake. A malicious web page visited in the same browser session can silently connect to the local WebSocket server and send arbitrary `DirectorCommand` payloads, allowing full remote control of the teleprompter content. Version 1.5.1 fixes the issue.	7.6	More Details
CVE-2026-28136	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VeronaLabs WP SMS wp-sms allows SQL Injection.This issue affects WP SMS: from n/a through <= 6.9.12.	7.6	More Details
CVE-2025-14343	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dokuzsoft Technology Ltd. E-Commerce Product allows Reflected XSS.This issue affects E-Commerce Product: through 10122025.	7.6	More Details
CVE-2025-69765	Tenda AX3 firmware v16.03.12.11 contains a stack overflow in formGetIptv function and the list parameter, which can cause memory corruption and enable remote code execution.	7.5	More Details
CVE-2026-27449	Umbraco Engage is a business intelligence platform. A vulnerability has been identified in Umbraco Engage prior to versions 16.2.1 and 17.1.1 where certain API endpoints are exposed without enforcing authentication or authorization checks. The affected endpoints can be accessed directly over the network without requiring a valid session or user credentials. By supplying a user-controlled identifier parameter (e.g., ?id=), an attacker can retrieve sensitive data associated with arbitrary records. Because no access control validation is performed, the endpoints are vulnerable to enumeration attacks, allowing attackers to iterate over identifiers and extract data at scale. An unauthenticated attacker can retrieve sensitive Engage-related data by directly querying the affected API endpoints. The vulnerability allows arbitrary record access through predictable or enumerable identifiers. The confidentiality impact is considered high. No direct integrity or availability impact has been identified. The scope of exposed data depends on the deployment but may include analytics data, tracking data, customer-related information, or other Engage-managed content. The vulnerability affects both v16 and v17. Patches have already been released. Users are advised to update to 16.2.1 or 17.1.1. No known workarounds are available.	7.5	More Details
CVE-2026-26078	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, when the `patreon_webhook_secret` site setting is blank, an attacker can forge valid webhook signatures by computing an HMAC-MD5 with an empty string as the key. Since the request body is known to the sender, the attacker can produce a matching signature and send arbitrary webhook payloads. This allows unauthorized creation, modification, or deletion of Patreon pledge data and triggering patron-to-group synchronization. This vulnerability is patched in versions 2025.12.2, 2026.1.1, and 2026.2.0. The fix rejects webhook requests when the webhook secret is not configured, preventing signature forgery with an empty key. As a workaround, configure the `patreon_webhook_secret` site setting with a strong, non-empty secret value. When the secret is non-empty, an attacker cannot forge valid signatures without knowing the secret.	7.5	More Details
CVE-2026-27141	Due to missing nil check, sending 0x0a-0x0f HTTP/2 frames will cause a running server to panic	7.5	More Details
CVE-2026-27640	tfplan2md is software for converting Terraform plan JSON files into human-readable Markdown reports. Prior to version 1.26.1, a bug in tfplan2md affected several distinct rendering paths: AzApi resource body properties, AzureDevOps variable groups, Scriban template context variables, and hierarchical sensitivity detection. This caused reports to render values that should have been masked as "(sensitive)" instead. This issue is fixed in v1.26.1. No known workarounds are available.	7.5	More Details

CVE-2026-26265	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, an IDOR vulnerability in the directory items endpoint allows any user, including anonymous users, to retrieve private user field values for all users in the directory. The `user_field_ids` parameter in `DirectoryItemsController#index` accepts arbitrary user field IDs without authorization checks, bypassing the visibility restrictions (`show_on_profile` / `show_on_user_card`) that are enforced elsewhere (e.g., `UserCardSerializer` via `Guardian#allowed_user_field_ids`). An attacker can request `GET /directory_items.json?period=all&user_field_ids=<id>` with any private field ID and receive that field's value for every user in the directory response. This enables bulk exfiltration of private user data such as phone numbers, addresses, or other sensitive custom fields that admins have explicitly configured as non-public. The issue is patched in versions 2025.12.2, 2026.1.1, and 2026.2.0 by filtering `user_field_ids` against `UserField.public_fields` for non-staff users before building the custom field map. As a workaround, site administrators can remove sensitive data from private user fields, or disable the user directory via the `enable_user_directory` site setting.	7.5	More Details
CVE-2026-27932	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. In 1.6.2 and earlier, a resource exhaustion vulnerability in joserfc allows an unauthenticated attacker to cause a Denial of Service (DoS) via CPU exhaustion. When the library decrypts a JSON Web Encryption (JWE) token using Password-Based Encryption (PBES2) algorithms, it reads the p2c (PBES2 Count) parameter directly from the token's protected header. This parameter defines the number of iterations for the PBKDF2 key derivation function. Because joserfc does not validate or bound this value, an attacker can specify an extremely large iteration count (e.g., 2^31 - 1), forcing the server to expend massive CPU resources processing a single token. This vulnerability exists at the JWA layer and impacts all high-level JWE and JWT decryption interfaces if PBES2 algorithms are allowed by the application's policy.	7.5	More Details
CVE-2026-22205	SPIP versions prior to 4.4.10 contain an authentication bypass vulnerability caused by PHP type juggling that allows unauthenticated attackers to access protected information. Attackers can exploit loose type comparisons in authentication logic to bypass login verification and retrieve sensitive internal data.	7.5	More Details
CVE-2026-27888	pypdf is a free and open-source pure-python PDF library. Prior to 6.7.3, an attacker who uses this vulnerability can craft a PDF which leads to the RAM being exhausted. This requires accessing the `xfa` property of a reader or writer and the corresponding stream being compressed using `/FlateDecode`. This has been fixed in pypdf 6.7.3. As a workaround, apply the patch manually.	7.5	More Details
CVE-2026-25945	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-24445	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-27942	fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. Prior to version 5.3.8, the application crashes with stack overflow when user use XML builder with `preserveOrder:true`. Version 5.3.8 fixes the issue. As a workaround, use XML builder with `preserveOrder:false` or check the input data before passing to builder.	7.5	More Details
CVE-2026-27959	Koa is middleware for Node.js using ES2017 async functions. Prior to versions 3.1.2 and 2.16.4, Koa's `ctx.hostname` API performs naive parsing of the HTTP Host header, extracting everything before the first colon without validating the input conforms to RFC 3986 hostname syntax. When a malformed Host header containing a `@` symbol is received, `ctx.hostname` returns `evil[.]com` - an attacker-controlled value. Applications using `ctx.hostname` for URL generation, password reset links, email verification URLs, or routing decisions are vulnerable to Host header injection attacks. Versions 3.1.2 and 2.16.4 fix the issue.	7.5	More Details
CVE-2026-3338	Improper signature validation in PKCS7_verify() in AWS-LC allows an unauthenticated user to bypass signature verification when processing PKCS7 objects with Authenticated Attributes. Customers of AWS services do not need to take action. Applications using AWS-LC should upgrade to AWS-LC version 1.69.0.	7.5	More Details

CVE-2026-25113	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-2597	Crypt::SysRandom::XS versions before 0.010 for Perl is vulnerable to a heap buffer overflow in the XS function random_bytes(). The function does not validate that the length parameter is non-negative. If a negative value (e.g. -1) is supplied, the expression length + 1u causes an integer wraparound, resulting in a zero-byte allocation. The subsequent call to chosen random function (e.g. getrandom) passes the original negative value, which is implicitly converted to a large unsigned value (typically SIZE_MAX). This can result in writes beyond the allocated buffer, leading to heap memory corruption and application crash (denial of service). In common usage, the length argument is typically hardcoded by the caller, which reduces the likelihood of attacker-controlled exploitation. Applications that pass untrusted input to this parameter may be affected.	7.5	More Details
CVE-2026-20792	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or misrouting legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-3336	Improper certificate validation in PKCS7_verify() in AWS-LC allows an unauthenticated user to bypass certificate chain verification when processing PKCS7 objects with multiple signers, except the final signer. Customers of AWS services do not need to take action. Applications using AWS-LC should upgrade to AWS-LC version 1.69.0.	7.5	More Details
CVE-2026-27595	Parse Dashboard is a standalone dashboard for managing Parse Server apps. In versions 7.3.0-alpha.42 through 9.0.0-alpha.7, the AI Agent API endpoint (POST `/apps/:appId/agent`) has multiple security vulnerabilities that, when chained, allow unauthenticated remote attackers to perform arbitrary read and write operations against any connected Parse Server database using the master key. The agent feature is opt-in; dashboards without an agent config are not affected. The fix in version 9.0.0-alpha.8 adds authentication, CSRF validation, and per-app authorization middleware to the agent endpoint. Read-only users are restricted to the `readOnlyMasterKey` with write permissions stripped server-side. A cache key collision between master key and read-only master key was also corrected. As a workaround, remove or comment out the agent configuration block from your Parse Dashboard configuration.	7.5	More Details
CVE-2026-1557	The WP Responsive Images plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.0 via the 'src' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2026-27904	minimatch is a minimal matching utility for converting glob expressions into JavaScript RegExp objects. Prior to version 10.2.3, 9.0.7, 8.0.6, 7.4.8, 6.2.2, 5.1.8, 4.2.5, and 3.1.4, nested `*()` extglobs produce regexps with nested unbounded quantifiers (e.g. `(?:(?:a|b)*)*`), which exhibit catastrophic backtracking in V8. With a 12-byte pattern `*(*(*(a|b)))` and an 18-byte non-matching input, `minimatch()` stalls for over 7 seconds. Adding a single nesting level or a few input characters pushes this to minutes. This is the most severe finding: it is triggered by the default `minimatch()` API with no special options, and the minimum viable pattern is only 12 bytes. The same issue affects `+()` extglobs equally. Versions 10.2.3, 9.0.7, 8.0.6, 7.4.8, 6.2.2, 5.1.8, 4.2.5, and 3.1.4 fix the issue.	7.5	More Details
CVE-2026-27903	minimatch is a minimal matching utility for converting glob expressions into JavaScript RegExp objects. Prior to version 10.2.3, 9.0.7, 8.0.6, 7.4.8, 6.2.2, 5.1.8, 4.2.5, and 3.1.3, `matchOne()` performs unbounded recursive backtracking when a glob pattern contains multiple non-adjacent `**` (GLOBSTAR) segments and the input path does not match. The time complexity is O(C(n, k)) -- binomial -- where `n` is the number of path segments and `k` is the number of globstars. With k=11 and n=30, a call to the default `minimatch()` API stalls for roughly 5 seconds. With k=13, it exceeds 15 seconds. No memoization or call budget exists to bound this behavior. Any application where an attacker can influence the glob pattern passed to `minimatch()` is vulnerable. The realistic attack surface includes build tools and task runners that accept user-supplied glob arguments (ESLint, Webpack, Rollup config), multi-tenant systems where one tenant configures glob-based rules that run in a shared process, admin or developer interfaces that accept ignore-rule or filter configuration as globs, and CI/CD pipelines that evaluate user-submitted config files containing glob patterns. An attacker who can place a crafted pattern into any of these paths can stall the Node.js event loop for tens of seconds per invocation. The pattern is 56 bytes for a 5-second stall and does not require authentication in contexts where pattern input is part of the feature. Versions 10.2.3, 9.0.7, 8.0.6, 7.4.8, 6.2.2, 5.1.8, 4.2.5, and 3.1.3 fix the issue.	7.5	More Details

CVE-2026-28276	Initiative is a self-hosted project management platform. An access control vulnerability exists in Initiative versions prior to 0.32.2 where uploaded documents are served from a publicly accessible /uploads/ directory without any authentication or authorization checks. Any uploaded file can be accessed directly via its URL by unauthenticated users (e.g., in an incognito browser session), leading to potential disclosure of sensitive documents. The problem was patched in v0.32.2, and the patch was further improved on in 032.4.	7.5	More Details
CVE-2026-27628	pypdf is a free and open-source pure-python PDF library. Prior to 6.7.2, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires reading the file. This has been fixed in pypdf 6.7.2. As a workaround, one may apply the patch manually.	7.5	More Details
CVE-2026-25673	An issue was discovered in 6.0 before 6.0.3, 5.2 before 5.2.12, and 4.2 before 4.2.29. `URLField.to_python()` in Django calls `urllib.parse.urlsplit()`, which performs NFKC normalization on Windows that is disproportionately slow for certain Unicode characters, allowing a remote attacker to cause denial of service via large URL inputs containing these characters. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Seokchan Yoon for reporting this issue.	7.5	More Details
CVE-2026-25114	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-20434	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: MOLY00782946; Issue ID: MSV-4135.	7.5	More Details
CVE-2026-27635	Manyfold is an open source, self-hosted web application for managing a collection of 3d models, particularly focused on 3d printing. Prior to version 0.133.0, when model render generation is enabled, a logged-in user can achieve RCE by uploading a ZIP containing a file with a shell metacharacter in its name. The filename reaches a Ruby backtick call unsanitized. Version 0.133.0 fixes the issue.	7.5	More Details
CVE-2026-27831	rldns is an open source DNS server. Version 1.3 has a heap-based out-of-bounds read that leads to denial of service. Version 1.4 contains a patch for the issue.	7.5	More Details
CVE-2026-3180	The Contest Gallery – Upload & Vote Photos, Media, Sell with PayPal & Stripe plugin for WordPress is vulnerable to blind SQL Injection via the ‘cgLostPasswordEmail’ and the ’cgl_mail’ parameter in all versions up to, and including, 28.1.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The vulnerability's ‘cgLostPasswordEmail’ parameter was patched in version 28.1.4, and the ’cgl_mail’ parameter was patched in version 28.1.5.	7.5	More Details
CVE-2026-25954	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_rail_server_local_move_size` dereferences a freed `xfAppWindow` pointer because `xf_rail_get_window` returns an unprotected pointer from the `railWindows` hash table, and the main thread can concurrently delete the window (via a window delete order) while the RAIL channel thread is still using the pointer. Version 3.23.0 fixes the issue.	7.5	More Details
CVE-2026-25942	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_rail_server_execute_result` indexes the global `error_code_names[]` array (7 elements, indices 0–6) with an unchecked `execResult->execResult` value received from the server, allowing an out-of-bounds read when the server sends an `execResult` value of 7 or greater. Version 3.23.0 fixes the issue.	7.5	More Details
CVE-2025-50180	esm.sh is a no-build content delivery network (CDN) for web development. In version 136, esm.sh is vulnerable to a full-response SSRF, allowing an attacker to retrieve information from internal websites through the vulnerability. Version 137 fixes the vulnerability.	7.5	More Details
CVE-2026-1662	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.4 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have allowed an unauthenticated user to cause Denial of Service by sending specially crafted requests to the Jira events endpoint.	7.5	More Details

CVE-2026-1388	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.2 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have allowed an unauthenticated user to cause regular expression denial of service by sending specially crafted input to a merge request endpoint under certain conditions.	7.5	More Details
CVE-2025-14511	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.2 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have allowed an unauthenticated user to cause denial of service by sending specially crafted files to the container registry event endpoint under certain conditions.	7.5	More Details
CVE-2026-28400	Docker Model Runner (DMR) is software used to manage, run, and deploy AI models using Docker. Versions prior to 1.0.16 expose a POST `/engines/_configure` endpoint that accepts arbitrary runtime flags without authentication. These flags are passed directly to the underlying inference server (llama.cpp). By injecting the --log-file flag, an attacker with network access to the Model Runner API can write or overwrite arbitrary files accessible to the Model Runner process. When bundled with Docker Desktop (where Model Runner is enabled by default since version 4.46.0), it is reachable from any default container at model-runner.docker.internal without authentication. In this context, the file overwrite can target the Docker Desktop VM disk (`Docker.raw`), resulting in the destruction of all containers, images, volumes, and build history. However, in specific configurations and with user interaction, it is possible to convert this vulnerability in a container escape. The issue is fixed in Docker Model Runner 1.0.16. Docker Desktop users should update to 4.61.0 or later, which includes the fixed Model Runner. A workaround is available. For Docker Desktop users, enabling Enhanced Container Isolation (ECI) blocks container access to Model Runner, preventing exploitation. However, if the Docker Model Runner is exposed to localhost over TCP in specific configurations, the vulnerability is still exploitable.	7.5	More Details
CVE-2026-28414	Gradio is an open-source Python package designed for quick prototyping. Prior to version 6.7, Gradio apps running on Window with Python 3.13+ are vulnerable to an absolute path traversal issue that enables unauthenticated attackers to read arbitrary files from the file system. Python 3.13+ changed the definition of `os.path.isabs` so that root-relative paths like `/windows/win.ini` on Windows are no longer considered absolute paths, resulting in a vulnerability in Gradio's logic for joining paths safely. This can be exploited by unauthenticated attackers to read arbitrary files from the Gradio server, even when Gradio is set up with authentication. Version 6.7 fixes the issue.	7.5	More Details
CVE-2026-27730	esm.sh is a no-build content delivery network (CDN) for web development. Versions up to and including 137 have an SSRF vulnerability (CWE-918) in esm.sh's `/http(s)` fetch route. The service tries to block localhost/internal targets, but the validation is based on hostname string checks and can be bypassed using DNS alias domains. This allows an external requester to make the esm.sh server fetch internal localhost services. As of time of publication, no known patched versions exist.	7.5	More Details
CVE-2026-2471	The WP Mail Logging plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.15.0 via deserialization of untrusted input from the email log message field. This is due to the `BaseModel` class constructor calling `maybe_unserialize()` on all properties retrieved from the database without validation. This makes it possible for unauthenticated attackers to inject a PHP Object by submitting a double-serialized payload through any public-facing form that sends email (e.g., Contact Form 7). When the email is logged and subsequently viewed by an administrator, the malicious payload is deserialized into an arbitrary PHP object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	7.5	More Details
CVE-2025-13673	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to SQL Injection via the 'coupon_code' parameter in all versions up to, and including, 3.9.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. NOTE: This vulnerability was partially mitigated in versions 3.9.4 and 3.9.6.	7.5	More Details
	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the session expiration check in `library/auth.inc.php` runs only when `skip_timeout_reset` is not present in the request. When `skip_timeout_reset=1` is sent,		

CVE-2026-25476	the entire block that calls `SessionTracker::isSessionExpired()` and forces logout on timeout is skipped. As a result, any request that includes this parameter (e.g. from auto-refresh pages like the Patient Flow Board) never runs the expiration check: expired sessions can continue to access data indefinitely, abandoned workstations stay active, and an attacker with a stolen session cookie can keep sending `skip_timeout_reset=1` to avoid being logged out. Version 8.0.0 fixes the issue.	7.5	More Details
CVE-2026-20128	A vulnerability in the Data Collection Agent (DCA) feature of Cisco Catalyst SD-WAN Manager could allow an authenticated, local attacker to gain DCA user privileges on an affected system. To exploit this vulnerability, the attacker must have valid vmanage credentials on the affected system. This vulnerability is due to the presence of a credential file for the DCA user on an affected system. An attacker could exploit this vulnerability by accessing the filesystem as a low-privileged user and reading the file that contains the DCA password from that affected system. A successful exploit could allow the attacker to access another affected system and gain DCA user privileges. Note: Cisco Catalyst SD-WAN Manager releases 20.18 and later are not affected by this vulnerability.	7.5	More Details
CVE-2025-58107	In Microsoft Exchange through 2019, Exchange ActiveSync (EAS) configurations on on-premises servers may transmit sensitive data from Samsung mobile devices in cleartext, including the user's name, e-mail address, device ID, bearer token, and base64-encoded password.	7.5	More Details
CVE-2026-27850	Due to an improperly configured firewall rule, the router will accept any connection on the WAN port with the source port 5222, exposing all services which are normally only accessible through the local network. This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	7.5	More Details
CVE-2025-70252	An issue was discovered in /goform/WifiWpsStart in Tenda AC6V2.0 V15.03.06.23_multi. The index and mode are controllable. If the conditions are met to sprintf, they will be spliced into tmp. It is worth noting that there is no size check,which leads to a stack overflow vulnerability.	7.5	More Details
CVE-2026-27836	phpMyFAQ is an open source FAQ web application. Prior to version 4.0.18, the WebAuthn prepare endpoint (`/api/webauthn/prepare`) creates new active user accounts without any authentication, CSRF protection, captcha, or configuration checks. This allows unauthenticated attackers to create unlimited user accounts even when registration is disabled. Version 4.0.18 fixes the issue.	7.5	More Details
CVE-2026-2428	The Fluent Forms Pro Add On Pack plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in all versions up to, and including, 6.1.17. This is due to the PayPal IPN (Instant Payment Notification) verification being disabled by default (`disable_ipn_verification` defaults to `'yes'` in `PayPalSettings.php`). This makes it possible for unauthenticated attackers to send forged PayPal IPN notifications to the publicly accessible IPN endpoint, marking unpaid form submissions as "paid" and triggering post-payment automation (emails, access grants, digital product delivery).	7.5	More Details
CVE-2026-27950	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, the fix for the heap-use-after-free described in CVE-2026-24680 is incomplete. While the vulnerable execution flow referenced in the advisory exists in the SDL2 implementation, the fix appears to have been applied only to the SDL3 code path. In the SDL2 implementation, the pointer is not nulled after free. This creates a situation where the advisory suggests the vulnerability is fully resolved, while builds or environments still using SDL2 may retain the vulnerable logic. A complete fix is available in version 3.23.0.	7.5	More Details
CVE-2026-26305	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-27633	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. Versions prior to version 2.02 have a Denial of Service (DoS) vulnerability via memory exhaustion. Unauthenticated remote attackers can send an HTTP POST request to the server with an exceptionally large `Content-Length` header (e.g., `2147483647`). The server continuously allocates memory for the request body (`EntityBody`) while streaming the payload without enforcing any maximum limit, leading to all available memory being consumed and causing the server to crash. Anyone hosting services using TinyWeb is impacted. Version 2.02 fixes the issue. The patch introduces a `CMaxEntityBodySize` limit (set to 10MB) for the maximum size of accepted payloads. As a temporary workaround if upgrading is not immediately possible, consider placing the server behind a Web Application Firewall (WAF) or reverse proxy (like nginx or Cloudflare) configured to explicitly limit the maximum allowed HTTP request body size (e.g., `client_max_body_size` in	7.5	More Details

	nginx).		
CVE-2026-27630	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. Versions prior to version 2.02 are vulnerable to a Denial of Service (DoS) attack known as Slowloris. The server spawns a new OS thread for every incoming connection without enforcing a maximum concurrency limit or an appropriate request timeout. An unauthenticated remote attacker can exhaust server concurrency limits and memory by opening numerous connections and sending data exceptionally slowly (e.g. 1 byte every few minutes). Anyone hosting services using TinyWeb is impacted. Version 2.02 fixes the issue. The patch introduces a `CMaxConnections` limit (set to 512) and a `CConnectionTimeoutSecs` idle timeout (set to 30 seconds). As a temporary workaround if upgrading is not immediately possible, consider placing the server behind a robust reverse proxy or Web Application Firewall (WAF) such as nginx, HAProxy, or Cloudflare, configured to buffer incomplete requests and aggressively enforce connection limits and timeouts.	7.5	More Details
CVE-2025-10990	A flaw was found in REXML. A remote attacker could exploit inefficient regular expression (regex) parsing when processing hex numeric character references (&#x...;) in XML documents. This could lead to a Regular Expression Denial of Service (ReDoS), impacting the availability of the affected component. This issue is the result of an incomplete fix for CVE-2024-49761.	7.5	More Details
CVE-2026-1916	The WPGSI: Spreadsheet Integration plugin for WordPress is vulnerable to unauthorized modification and loss of data due to missing capability checks and an insecure authentication mechanism on the `wpgsi_callBackFuncAccept` and `wpgsi_callBackFuncUpdate` REST API functions in all versions up to, and including, 3.8.3. Both REST endpoints use `permission_callback => '__return_true'`, allowing unauthenticated access. The plugin's custom token-based validation relies on a Base64-encoded JSON object containing the user ID and email address, but is not cryptographically signed. This makes it possible for unauthenticated attackers to forge tokens using publicly enumerable information (admin user ID and email) to create, modify, and delete arbitrary WordPress posts and pages, granted they know the administrator's email address and an active integration ID with remote updates enabled.	7.5	More Details
CVE-2026-2416	The Geo Mashup plugin for WordPress is vulnerable to SQL Injection via the 'sort' parameter in all versions up to, and including, 1.13.17. 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 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-2026-2252	An XML External Entity (XXE) vulnerability allows malicious user to perform Server-Side Request Forgery (SSRF) via crafted XML input containing malicious external entity references. This issue affects Xerox FreeFlow Core versions up to and including 8.0.7. Please consider upgrading to FreeFlow Core version 8.1.0 via the software available on - https://www.support.xerox.com/en-us/product/core/downloads	7.5	More Details
CVE-2026-26986	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `rail_window_free` dereferences a freed `xfAppWindow` pointer during `HashTable_Free` cleanup because `xf_rail_window_common` calls `free(appWindow)` on title allocation failure without first removing the entry from the `railWindows` hash table, leaving a dangling pointer that is freed again on disconnect. Version 3.23.0 fixes the vulnerability.	7.5	More Details
CVE-2026-20051	A vulnerability with the Ethernet VPN (EVPN) Layer 2 ingress packet processing of Cisco Nexus 3600 Platform Switches and Cisco Nexus 9500-R Series Switching Platforms could allow an unauthenticated, adjacent attacker to trigger a Layer 2 traffic loop. This vulnerability is due to a logic error when processing a crafted Layer 2 ingress frame. An attacker could exploit this vulnerability by sending a stream of crafted Ethernet frames through the targeted device. A successful exploit could allow the attacker to cause a Layer 2 Virtual eXtensible LAN (VxLAN) traffic loop, which, in turn, could result in a denial of service (DoS) condition. This Layer 2 loop could oversubscribe the bandwidth on network interfaces, which would result in all data plane traffic being dropped. To exploit this vulnerability, the attacker must be Layer 2-adjacent to the affected device. Note: To stop active exploitation of this vulnerability, manual intervention is required to both stop the crafted traffic and flap all involved network interfaces. For additional assistance if a Layer 2 loop that is related to this vulnerability is suspected, contact the Cisco Technical Assistance Center (TAC) or the proper support provider.	7.4	More Details
CVE-2025-48577	In multiple functions of KeyguardViewMediator.java, there is a possible lockscreen bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details

CVE-2026-27981	HomeBox is a home inventory and organization system. Prior to 0.24.0, the authentication rate limiter (authRateLimiter) tracks failed attempts per client IP. It determines the client IP by reading, 1. X-Real-IP header, 2. First entry of X-Forwarded-For header, and 3. r.RemoteAddr (TCP connection address). These headers were read unconditionally. An attacker connecting directly to Homebox could forge any value in X-Real-IP, effectively getting a fresh rate limit identity per request. There is a TrustProxy option in the configuration (Options.TrustProxy, default false), but this option was never read by any middleware or rate limiter code. Additionally, chi's middleware.RealIP was applied unconditionally in main.go, overwriting r.RemoteAddr with the forged header value before it reaches any handler. This vulnerability is fixed in 0.24.0.	7.4	More Details
CVE-2026-27800	Zed, a code editor, has a Zip Slip (Path Traversal) vulnerability exists in its extension archive extraction functionality prior to version 0.224.4. The `extract_zip()` function in `crates/util/src/archive.rs` fails to validate ZIP entry filenames for path traversal sequences (e.g., `../`). This allows a malicious extension to write files outside its designated sandbox directory by downloading and extracting a crafted ZIP archive. Version 0.224.4 fixes the issue.	7.4	More Details
CVE-2025-48630	In drawLayersInternal of SkiaRenderEngine.cpp, there is a possible way to access the GPU cache due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details
CVE-2026-20033	A vulnerability in Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation when processing specific Ethernet frames. An attacker could exploit this vulnerability by sending a crafted Ethernet frame to the management interface of an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. Note: Only the out-of-band (OOB) management interface is affected.	7.4	More Details
CVE-2026-20010	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the LLDP process to restart, which could cause an affected device to reload unexpectedly. This vulnerability is due to improper handling of specific fields in an LLDP frame. An attacker could exploit this vulnerability by sending a crafted LLDP packet to an interface of an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition. Note: LLDP is a Layer 2 link protocol. To exploit this vulnerability, an attacker would need to be directly connected to an interface of an affected device, either physically or logically (for example, through a Layer 2 Tunnel configured to transport the LLDP protocol).	7.4	More Details
CVE-2025-48568	In multiple locations, there is a possible lockscreen bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details
CVE-2026-28372	telnetd in GNU inetutils through 2.7 allows privilege escalation that can be exploited by abusing systemd service credentials support added to the login(1) implementation of util-linux in release 2.40. This is related to client control over the CREDENTIALS_DIRECTORY environment variable, and requires an unprivileged local user to create a login.noauth file.	7.4	More Details
CVE-2026-27652	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3413	A flaw has been found in itsourcecode University Management System 1.0. This vulnerability affects unknown code of the file /admin_single_student.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-20895	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by	7.3	More Details

	overwhelming the backend with valid session requests.		
CVE-2026-3411	A security vulnerability has been detected in itsourcecode University Management System 1.0. Affected by this issue is some unknown functionality of the file /admin_single_student_update.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-3410	A weakness has been identified in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/check_studid.php. Executing a manipulation of the argument student_id can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-3409	A security flaw has been discovered in eosphoros-ai db-gpt 0.7.5. Affected is the function importlib.machinery.SourceFileLoader.exec_module of the file /api/v1/serve/awel/flow/import of the component Flow Import Endpoint. Performing a manipulation as part of File results in code injection. 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.	7.3	More Details
CVE-2026-3406	A vulnerability was found in projectworlds Online Art Gallery Shop 1.0. The impacted element is an unknown function of the file /admin/registration.php of the component Registration Handler. The manipulation of the argument fname results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-25906	Dell Optimizer, versions prior to 6.3.1, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	7.3	More Details
CVE-2026-27647	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3134	A security flaw has been discovered in itsourcecode News Portal Project 1.0. The affected element is an unknown function of the file /newsportal/admin/edit-category.php. The manipulation of the argument Category results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-25778	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3395	A flaw has been found in MaxSite CMS up to 109.1. This impacts the function eval of the file application/maxsite/admin/plugins/editor_markitup/preview-ajax.php of the component MarkItUp Preview AJAX Endpoint. Executing a manipulation can lead to code injection. It is possible to launch the attack remotely. The exploit has been published and may be used. Upgrading to version 109.2 will fix this issue. This patch is called 08937a3c5d672a242d68f53e9fccf8a748820ef3. You should upgrade the affected component. The code maintainer was informed beforehand about the issues. He reacted very fast and highly professional.	7.3	More Details
CVE-2026-27707	Seerr is an open-source media request and discovery manager for Jellyfin, Plex, and Emby. Starting in version 2.0.0 and prior to version 3.1.0, an authentication guard logic flaw in `POST /api/v1/auth/jellyfin` allows an unauthenticated attacker to register a new Seerr account on any Plex-configured instance by authenticating with an attacker-controlled Jellyfin server. The attacker receives an authenticated session and can immediately use the application with default permissions, including the ability to submit media requests to Radarr/Sonarr. Any Seerr deployment where all three of the following are true may be vulnerable: `settings.main.mediaServerType` is set to `PLEX` (the most common deployment).; `settings.jellyfin.ip` is set to `""` (default, meaning Jellyfin was never configured); and	7.3	More Details

	`settings.main.newPlexLogin` is set to `true` (default). Jellyfin-configured and Emby-configured deployments are not affected. Version 3.1.0 of Seerr fixes this issue.		
CVE-2026-25711	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2025-48634	In relayoutWindow of WindowManagerService.java, there is a possible tapjack attack due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.3	More Details
CVE-2026-3261	A flaw has been found in itsourcecode School Management System 1.0. This impacts an unknown function of the file /settings/index.php of the component Setting Handler. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-28279	osctrl is an osquery management solution. Prior to version 0.5.0, an OS command injection vulnerability exists in the `osctrl-admin` environment configuration. An authenticated administrator can inject arbitrary shell commands via the hostname parameter when creating or editing environments. These commands are embedded into enrollment one-liner scripts generated using Go's `text/template` package (which does not perform shell escaping) and execute on every endpoint that enrolls using the compromised environment. An attacker with administrator access can achieve remote code execution on every endpoint that enrolls using the compromised environment. Commands execute as root/SYSTEM (the privilege level used for osquery enrollment) before osquery is installed, leaving no agent-level audit trail. This enables backdoor installation, credential exfiltration, and full endpoint compromise. This is fixed in osctrl `v0.5.0`. As a workaround, restrict osctrl administrator access to trusted personnel, review existing environment configurations for suspicious hostnames, and/or monitor enrollment scripts for unexpected commands.	7.3	More Details
CVE-2026-26290	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3133	A vulnerability has been found in itsourcecode Document Management System 1.0. This issue affects some unknown processing of the file /loging.php of the component Login. The manipulation of the argument Username leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-3153	A vulnerability has been found in itsourcecode Document Management System 1.0. Impacted is an unknown function of the file /register.php. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-3151	A vulnerability was detected in itsourcecode College Management System 1.0. This vulnerability affects unknown code of the file /login/login.php. The manipulation of the argument email results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-3152	A flaw has been found in itsourcecode College Management System 1.0. This issue affects some unknown processing of the file /admin/teacher-salary.php. This manipulation of the argument teacher_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-	Vikunja is an open-source self-hosted task management platform. Prior to version 2.0.0, the application allows users to upload SVG files as task attachments. SVG is an XML-based format that supports JavaScript execution through elements such as <script> tags or event handlers like onload. The application does not sanitize SVG content before storing it. When the uploaded SVG	7.3	More

27616	file is accessed via its direct URL, it is rendered inline in the browser under the application's origin. As a result, embedded JavaScript executes in the context of the authenticated user. Because the authentication token is stored in localStorage, it is accessible via JavaScript and can be retrieved by a malicious payload. Version 2.0.0 patches this issue.		Details
CVE-2026-3200	A vulnerability was identified in z-9527 admin 1.0/2.0. The affected element is the function checkName/register/login/getUser/getUsers of the file /server/controller/user.js. The manipulation leads to sql injection. The attack 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.	7.3	More Details
CVE-2026-3164	A vulnerability was found in itsourcecode News Portal Project 1.0. This issue affects some unknown processing of the file /admin/contactus.php. The manipulation of the argument pagetitle results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-3135	A weakness has been identified in itsourcecode News Portal Project 1.0. The impacted element is an unknown function of the file /admin/add-category.php. This manipulation of the argument Category causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-3148	A vulnerability was determined in SourceCodester Simple and Nice Shopping Cart Script 1.0. This impacts an unknown function of the file /signup.php. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-25733	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Custom Rules function of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	7.3	More Details
CVE-2025-50197	Chamilo is a learning management system. Prior to version 1.11.30, there is an OS Command Injection vulnerability in /main/admin/sub_language_ajax.inc.php via the POST new_language parameter. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2025-50196	Chamilo is a learning management system. Prior to version 1.11.30, there is an OS Command Injection vulnerability in /plugin/vchamilo/views/editinstance.php via the POST main_database parameter. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2025-50195	Chamilo is a learning management system. Prior to version 1.11.30, there is an OS Command Injection vulnerability in /plugin/vchamilo/views/manage.controller.php. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2025-50194	Chamilo is a learning management system. Prior to version 1.11.30, there is an OS Command Injection vulnerability in /main/cron/lang/check_parse_lang.php. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2026-2269	The Uncanny Automator – Easy Automation, Integration, Webhooks & Workflow Builder Plugin plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.0.0.3 via the download_url() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. Additionally, the plugin stores the contents of the remote files on the server, which can be leveraged to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-50191	Chamilo is a learning management system. Prior to version 1.11.30, there is an error-based SQL Injection via POST userFile with the /main/exercise/hotpotatoes.php script. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2025-47383	Weak configuration may lead to cryptographic issue when a VoWiFi call is triggered from UE.	7.2	More Details

CVE-2025-63909	Incorrect access control in the component /opt/SRLtzm/bin/TapeDumper of Cohesity TranZman Migration Appliance Release 4.0 Build 14614 allows attackers to escalate privileges to root and read and write arbitrary files.	7.2	More Details
CVE-2025-50188	Chamilo is a learning management system. Prior to version 1.11.30, the application performs insufficient validation of data coming from the user from the GET value parameter with the following scripts: /plugin/vchamilo/views/syncparams.php and /plugin/vchamilo/ajax/service.php, which allows an attacker to perform an attack aimed at modifying the database query logic by injecting an arbitrary SQL statements. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2024-47886	Chamilo is a learning management system. Chamillo is affected by a post-authentication phar unserialize which leads to a remote code execution (RCE) within versions 1.11.12 to 1.11.26. By abusing multiple supported features from the virtualization plugin vchamilo, the vulnerability allows an administrator to execute arbitrary code on the server. This issue has been patched in version 1.11.26.	7.2	More Details
CVE-2025-50193	Chamilo is a learning management system. Prior to version 1.11.30, there is an OS command Injection vulnerability in /plugin/vchamilo/views/import.php with the POST to_main_database parameter. This issue has been patched in version 1.11.30.	7.2	More Details
CVE-2025-63910	An authenticated arbitrary file upload vulnerability in Cohesity TranZman Migration Appliance Release 4.0 Build 14614 allows attackers with Administrator privileges to execute arbitrary code via uploading a crafted patch file.	7.2	More Details
CVE-2026-2568	The WP Zendesk for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form submission data in all versions up to, and including, 1.1.5 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-2026-27624	Coturn is a free open source implementation of TURN and STUN Server. Coturn is commonly configured to block loopback and internal ranges using "denied-peer-ip" and/or default loopback restrictions. CVE-2020-26262 addressed bypasses involving "0.0.0.0", "[::1]" and "[::]", but IPv4-mapped IPv6 is not covered. When sending a "CreatePermission" or "ChannelBind" request with the "XOR-PEER-ADDRESS" value of "::ffff:127.0.0.1", a successful response is received, even though "127.0.0.0/8" is blocked via "denied-peer-ip". The root cause is that, prior to the updated fix implemented in version 4.9.0, three functions in "src/client/ns_turn_ioaddr.c" do not check "IN6_IS_ADDR_V4MAPPED". "ioa_addr_is_loopback()" checks "127.x.x.x" (AF_INET) and "::1" (AF_INET6), but not "::ffff:127.0.0.1." "ioa_addr_is_zero()" checks "0.0.0.0" and "::", but not "::ffff:0.0.0.0." "addr_less_eq()" used by "ioa_addr_in_range()" for "denied-peer-ip" matching: when the range is AF_INET and the peer is AF_INET6, the comparison returns 0 without extracting the embedded IPv4. Version 4.9.0 contains an updated fix to address the bypass of the fix for CVE-2020-26262.	7.2	More Details
CVE-2026-20416	In pcie, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10315038 / ALPS10340155; Issue ID: MSV-5155.	7.2	More Details
CVE-2026-27819	Vikunja is an open-source self-hosted task management platform. Prior to version 2.0.0, the restoreConfig function in vikunja/pkg/modules/dump/restore.go of the go-vikunja/vikunja repository fails to sanitize file paths within the provided ZIP archive. A maliciously crafted ZIP can bypass the intended extraction directory to overwrite arbitrary files on the host system. Additionally, we've discovered that a malformed archive triggers a runtime panic, crashing the process immediately after the database has been wiped permanently. The application trusts the metadata in the ZIP archive. It uses the Name attribute of the zip.File struct directly in os.OpenFile calls without validation, allowing files to be written outside the intended directory. The restoration logic assumes a specific directory structure within the ZIP. When provided with a "minimalist" malicious ZIP, the application fails to validate the length of slices derived from the archive contents. Specifically, at line 154, the code attempts to access an index of len(ms)-2 on an insufficiently populated slice, triggering a panic. Version 2.0.0 fixes the issue.	7.2	More Details
CVE-2025-63911	Cohesity TranZman Migration Appliance Release 4.0 Build 14614 was discovered to contain an authenticated command injection vulnerability.	7.2	More Details

CVE-2026-28138	Deserialization of Untrusted Data vulnerability in Stylemix uListing ulisting allows Object Injection.This issue affects uListing: from n/a through <= 2.2.0.	7.2	More Details
CVE-2025-67840	Multiple authenticated OS command injection vulnerabilities exist in the Cohesity (formerly Stone Ram) TranZman 4.0 Build 14614 through TZM_1757588060_SEP2025_FULL.depot web application API endpoints (including Scheduler and Actions pages). The appliance directly concatenates user-controlled parameters into system commands without sufficient sanitisation, allowing an authenticated admin user to inject and execute arbitrary OS commands with root privileges. An attacker can intercept legitimate requests (e.g. during job creation or execution) using a proxy and modify parameters to include shell metacharacters, achieving remote code execution on the appliance. This completely bypasses the intended CLISH restricted shell confinement and results in full system compromise. The vulnerabilities persist in Release 4.0 Build 14614 including the latest patch (as of the time of testing) TZM_1757588060_SEP2025_FULL.depot.	7.2	More Details
CVE-2025-64427	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.5.0 and prior, due to insufficient validation or restriction of target URLs, an authenticated local user can craft requests that target internal IP addresses (e.g., 127.0.0.1, localhost, or private network ranges). This allows the attacker to interact with internal HTTP/HTTPS services that are not intended to be exposed externally or to local users. No known patch is publicly available.	7.1	More Details
CVE-2026-27638	Actual is a local-first personal finance tool. Prior to version 26.2.1, in multi-user mode (OpenID), the sync API endpoints (`/sync/*`) don't verify that the authenticated user owns or has access to the file being operated on. Any authenticated user can read, modify, and overwrite any other user's budget files by providing their file ID. Version 26.2.1 patches the issue.	7.1	More Details
CVE-2025-47378	Cryptographic Issue when a shared VM reference allows HLOS to boot loader and access cert chain.	7.1	More Details
CVE-2025-52469	Chamilo is a learning management system. Prior to version 1.11.30, a logic vulnerability in the friend request workflow of Chamilo’s social network module allows an authenticated user to forcibly add any user as a friend by directly calling the AJAX endpoint. The attacker can bypass the normal flow of sending and accepting friend requests, and even add non-existent users. This breaks access control and social interaction logic, with potential privacy implications. This issue has been patched in version 1.11.30.	7.1	More Details
CVE-2026-28402	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.2.2, a malicious or compromised validator that is elected as proposer can publish a macro block proposal where `header.body_root` does not match the actual macro body hash. The proposal can pass proposal verification because the macro proposal verification path validates the header but does not validate the binding `body_root == hash(body)`; later code expects this binding and may panic on mismatch, crashing validators. Note that the impact is only for validator nodes. The patch for this vulnerability is formally released as part of v1.2.2. The patch adds the corresponding body root verification in the proposal checks. No known workarounds are available.	7.1	More Details
CVE-2026-27692	iccDEV provides a set of libraries and tools for working with ICC color management profiles. In versions up to and including 2.3.1.4, heap-buffer-overflow read occurs during CIccTagTextDescription::Release() when strlen() reads past a heap buffer while parsing ICC profile XML text description tags, causing a crash. Commit 29d088840b962a7cdd35993dfabc2cb35a049847 fixes the issue. No known workarounds are available.	7.1	More Details
CVE-2026-25147	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, in `portal/portal_payment.php`, the patient id used for the page is taken from the request (`$pid = $_REQUEST['pid'] ?? $pid` and `$pid = ($_REQUEST['hidden_patient_code'] ?? null) > 0 ? $_REQUEST['hidden_patient_code'] : $pid`) instead of being fixed to the authenticated portal user. The portal session already has a valid `$pid` for the logged-in patient. Overwriting it with user-supplied values and using it without authorization allows a portal user to view and interact with another patient's demographics, invoices, and payment history—horizontal privilege escalation and IDOR. Version 8.0.0 contains a fix for the issue.	7.1	More Details
CVE-	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 An XML External Entity (XXE)		More

2026-1567	vulnerability in IBM InfoSphere Information Server could allow attackers to retrieve sensitive information from the server.	7.1	Details
CVE-2026-27967	Zed, a code editor, has a symlink escape vulnerability in versions prior to 0.225.9 in Agent file tools (`read_file`, `edit_file`). It allows reading and writing files **outside the project directory** when a project contains symbolic links pointing to external paths. This bypasses the intended workspace boundary and privacy protections (`file_scan_exclusions`, `private_files`), potentially leaking sensitive user data to the LLM. Version 0.225.9 fixes the issue.	7.1	More Details
CVE-2026-25927	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the DICOM viewer state API (e.g. upload or state save/load) accepts a document ID (`doc_id`) without verifying that the document belongs to the current user's authorized patient or encounter. An authenticated user can read or modify DICOM viewer state (e.g. annotations, view settings) for any document by enumerating document IDs. Version 8.0.0 fixes the issue.	7.1	More Details
CVE-2026-26103	A flaw was found in the udisks storage management daemon that exposes a privileged D-Bus API for restoring LUKS encryption headers without proper authorization checks. The issue allows a local unprivileged user to instruct the root-owned udisks daemon to overwrite encryption metadata on block devices. This can permanently invalidate encryption keys and render encrypted volumes inaccessible. Successful exploitation results in a denial-of-service condition through irreversible data loss.	7.1	More Details
CVE-2026-27757	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain an authentication vulnerability that allows authenticated users to change account passwords without verifying the current password. Attackers who gain access to an authenticated session can modify credentials to maintain persistent access to the management interface.	7.1	More Details
CVE-2026-25741	Zulip is an open-source team collaboration tool. Prior to commit bf28c82dc9b1f630fa8e9106358771b20a0040f7, the API endpoint for creating a card update session during an upgrade flow was accessible to users with only organization member privileges. When the associated Stripe Checkout session is completed, the Stripe webhook updates the organization's default payment method. Because no billing-specific authorization check is enforced, a regular (non-billing) member can change the organization's payment method. This vulnerability affected the Zulip Cloud payment processing system, and has been patched as of commit bf28c82dc9b1f630fa8e9106358771b20a0040f7. Self-hosted deploys are no longer affected and no patch or upgrade is required for them.	7.1	More Details
CVE-2025-48641	In multiple functions of Nfc.h, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2026-27933	Manyfold is an open source, self-hosted web application for managing a collection of 3d models, particularly focused on 3d printing. Versions prior to 0.133.0 are vulnerable to session hijack via cookie leakage in proxy caches. Version 0.133.0 fixes the issue.	6.8	More Details
CVE-2026-28423	Statmatic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.11 and 6.4.0, when Glide image manipulation is used in insecure mode (which is not the default), the image proxy can be abused by an unauthenticated user to make the server send HTTP requests to arbitrary URLs—either via the URL directly or via the watermark feature. That can allow access to internal services, cloud metadata endpoints, and other hosts reachable from the server. This has been fixed in 5.73.11 and 6.4.0.	6.8	More Details
CVE-2026-28338	PMD is an extensible multilanguage static code analyzer. Prior to version 7.22.0, PMD's `vbhtml` and `yahtml` report formats insert rule violation messages into HTML output without escaping. When PMD analyzes untrusted source code containing crafted string literals, the generated HTML report contains executable JavaScript that runs when opened in a browser. Practical impact is limited because `vbhtml` and `yahtml` are legacy formats rarely used in practice. The default `html` format is properly escaped and not affected. Version 7.22.0 contains a fix for the issue.	6.8	More Details
CVE-2026-20425	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5539.	6.7	More Details
CVE-2026-1585	An unquoted Windows service executable path vulnerability in IJ Scan Utility for Windows versions 1.1.2 through 1.5.0 may allow a local attacker to execute a malicious file with the privileges of the affected service.	6.7	More Details

CVE-2026-20440	In MAE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10431968; Issue ID: MSV-5824.	6.7	More Details
CVE-2026-20441	In MAE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10432500; Issue ID: MSV-5803.	6.7	More Details
CVE-2026-20428	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5536.	6.7	More Details
CVE-2026-20443	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10436998; Issue ID: MSV-5722.	6.7	More Details
CVE-2026-20099	A vulnerability in the web-based management interface of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation of command arguments supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of the affected device with root-level privileges.	6.7	More Details
CVE-2025-9909	A flaw was found in the Red Hat Ansible Automation Platform Gateway route creation component. This vulnerability allows credential theft via the creation of misleading routes using a double-slash (//) prefix in the gateway_path. A malicious or socially engineered administrator can configure a honey-pot route to intercept and exfiltrate user credentials, potentially maintaining persistent access or creating a backdoor even after their permissions are revoked.	6.7	More Details
CVE-2026-20427	In display, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5537.	6.7	More Details
CVE-2025-9908	A flaw was found in the Red Hat Ansible Automation Platform, Event-Driven Ansible (EDA) Event Streams. This vulnerability allows an authenticated user to gain access to sensitive internal infrastructure headers (such as X-Trusted-Proxy and X-Envoy-*) and event stream URLs via crafted requests and job templates. By exfiltrating these headers, an attacker could spoof trusted requests, escalate privileges, or perform malicious event injection.	6.7	More Details
CVE-2026-0027	In smmu_detach_dev of arm-smmu-v3.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-9907	A flaw was found in the Red Hat Ansible Automation Platform, Event-Driven Ansible (EDA) Event Stream API. This vulnerability allows exposure of sensitive client credentials and internal infrastructure headers via the test_headers field when an event stream is in test mode. The possible outcome includes leakage of internal infrastructure details, accidental disclosure of user or system credentials, privilege escalation if high-value tokens are exposed, and persistent sensitive data exposure to all users with read access on the event stream.	6.7	More Details
CVE-2026-20444	In display, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10436995; Issue ID: MSV-5721.	6.7	More Details
CVE-2026-20426	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5538.	6.7	More Details
CVE-2026-20436	In wlan STA driver, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00473802; Issue ID: MSV-5970.	6.7	More Details
	Zen C is a systems programming language that compiles to human-readable GNU C/C11. Prior to		

CVE-2026-28207	version 0.4.2, a command injection vulnerability (CWE-78) in the Zen C compiler allows local attackers to execute arbitrary shell commands by providing a specially crafted output filename via the `-o` command-line argument. The vulnerability existed in the `main` application logic (specifically in `src/main.c`), where the compiler constructed a shell command string to invoke the backend C compiler. This command string was built by concatenating various arguments, including the user-controlled output filename, and was subsequently executed using the `system()` function. Because `system()` invokes a shell to parse and execute the command, shell metacharacters within the output filename were interpreted by the shell, leading to arbitrary command execution. An attacker who can influence the command-line arguments passed to the `zc` compiler (like through a build script or a CI/CD pipeline configuration) can execute arbitrary commands with the privileges of the user running the compiler. The vulnerability has been fixed in version 0.4.2 by removing `system()` calls, implementing `ArgList`, and internal argument handling. Users are advised to update to Zen C version v0.4.2 or later.	6.6	More Details
CVE-2025-14604	IBM Storage Scale IBM S through rage Scale 5.2.3.0 - 5.2.3.5, and IBM S through rage Scale 6.0.0.0 - 6.0.0.1 could allow a local user to unintentionally trigger additional permissions for resources in a way that allows that resource to be executed by unintended actors.	6.6	More Details
CVE-2026-27711	NanaZip is an open source file archive. Starting in version 5.0.1252.0 and prior to versions 6.0.1638.0 and 6.5.1638.0, a memory corruption vulnerability in NanaZip's UFS parser allows a crafted `.ufs/.ufs2/.img` file to trigger out-of-bounds memory access during archive open/listing. The bug is reachable via normal user file-open flow and can cause process crash, hang, and potentially exploitable heap corruption. Versions 6.0.1638.0 and 6.5.1638.0 fix the issue.	6.6	More Details
CVE-2026-27794	LangGraph Checkpoint defines the base interface for LangGraph checkpointers. Prior to version 4.0.0, a Remote Code Execution vulnerability exists in LangGraph's caching layer when applications enable cache backends that inherit from `BaseCache` and opt nodes into caching via `CachePolicy`. Prior to `langgraph-checkpoint` 4.0.0, `BaseCache` defaults to `JsonPlusSerializer(pickle_fallback=True)`. When msgpack serialization fails, cached values can be deserialized via `pickle.loads(...)`. Caching is not enabled by default. Applications are affected only when the application explicitly enables a cache backend (for example by passing `cache=...` to `StateGraph.compile(...)` or otherwise configuring a `BaseCache` implementation), one or more nodes opt into caching via `CachePolicy`, and the attacker can write to the cache backend (for example a network-accessible Redis instance with weak/no auth, shared cache infrastructure reachable by other tenants/services, or a writable SQLite cache file). An attacker must be able to write attacker-controlled bytes into the cache backend such that the LangGraph process later reads and deserializes them. This typically requires write access to a networked cache (for example a network-accessible Redis instance with weak/no auth or shared cache infrastructure reachable by other tenants/services) or write access to local cache storage (for example a writable SQLite cache file via permissive file permissions or a shared writable volume). Because exploitation requires write access to the cache storage layer, this is a post-compromise / post-access escalation vector. LangGraph Checkpoint 4.0.0 patches the issue.	6.6	More Details
CVE-2026-27709	NanaZip is an open source file archive. Starting in version 5.0.1252.0 and prior to versions 6.0.1638.0 and 6.5.1638.0, NanaZip's `.NET Single File Application` parser has an out-of-bounds read vulnerability in manifest parsing. A crafted bundle can provide a malformed `RelativePathLength` so the parser constructs a `std::string` from memory beyond `HeaderBuffer`, leading to crash and potential in-process memory disclosure. Versions 6.0.1638.0 and 6.5.1638.0 fix the issue.	6.6	More Details
CVE-2026-2845	An issue has been discovered in GitLab CE/EE affecting all versions from 11.2 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have allowed an authenticated user to cause denial of service by exploiting a Bitbucket Server import endpoint via repeatedly sending large responses.	6.5	More Details
CVE-2026-20133	A vulnerability in Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to view sensitive information on an affected system. This vulnerability is due to insufficient file system access restrictions. An attacker could exploit this vulnerability by accessing the API of an affected system. A successful exploit could allow the attacker to read sensitive information on the underlying operating system.	6.5	More Details
CVE-2026-27943	OpenEMR is a free and open source electronic health records and medical practice management application. In versions up to and including 8.0.0, the eye exam (eye_mag) view loads data by `form_id` (or equivalent) without verifying that the form belongs to the current user's patient/encounter context. An authenticated user can access or edit any patient's eye exam by supplying another form ID; in some flows the session's active patient may also be switched. A fix	6.5	More Details

	is available on the `main` branch of the OpenEMR GitHub repository.		
CVE-2026-27773	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-28083	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UX-themes Flatsome flatsome allows Stored XSS.This issue affects Flatsome: from n/a through <= 3.20.1.	6.5	More Details
CVE-2021-4456	Net::CIDR versions before 0.24 for Perl mishandle leading zeros in IP CIDR addresses, which may have unspecified impact. The functions `addr2cidr` and `cidrlookup` may return leading zeros in a CIDR string, which may in turn be parsed as octal numbers by subsequent users. In some cases an attacker may be able to leverage this to bypass access controls based on IP addresses. The documentation advises validating untrusted CIDR strings with the `cidrvalidate` function. However, this mitigation is optional and not enforced by default. In practice, users may call `addr2cidr` or `cidrlookup` with untrusted input and without validation, incorrectly assuming that this is safe.	6.5	More Details
CVE-2026-3118	A security flaw was identified in the Orchestrator Plugin of Red Hat Developer Hub (Backstage). The issue occurs due to insufficient input validation in GraphQL query handling. An authenticated user can inject specially crafted input into API requests, which disrupts backend query processing. This results in the entire Backstage application crashing and restarting, leading to a platform-wide Denial of Service (DoS). As a result, legitimate users temporarily lose access to the platform.	6.5	More Details
CVE-2026-27954	Live Helper Chat is an open-source application that enables live support websites. In versions up to and including 4.52, three chat action endpoints (holdaction.php, blockuser.php, and transferchat.php) load chat objects by ID without calling `erLhcoreClassChat::hasAccessToRead()`, allowing operators to act on chats in departments they are not assigned to. Operators with the relevant role permissions (holduse, allowblockusers, allowtransfer) can hold, block users from, or transfer chats in departments they are not assigned to. This is a horizontal privilege escalation within one organization. As of time of publication, no known patched versions are available.	6.5	More Details
CVE-2026-24488	OpenEMR is a free and open source electronic health records and medical practice management application. In versions up to and including 8.0.0, an arbitrary file exfiltration vulnerability in the fax sending endpoint allows any authenticated user to read and transmit any file on the server (including database credentials, patient documents, system files, and source code) via fax to an attacker-controlled phone number. The vulnerability exists because the endpoint accepts arbitrary file paths from user input and streams them to the fax gateway without path restrictions or authorization checks. As of time of publication, no known patched versions are available.	6.5	More Details
CVE-2026-27753	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain an authentication bypass vulnerability that allows remote attackers to perform unlimited login attempts against the management interface. Attackers can conduct online password guessing attacks without account lockout or rate limiting restrictions to gain unauthorized access to the device management interface.	6.5	More Details
CVE-2026-27015	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, a missing bounds check in `smartcard_unpack_read_size_align()` (`libfreerdp/utils/smartcard_pack.c:1703`) allows a malicious RDP server to crash the FreeRDP client via a reachable `WINPR_ASSERT` → `abort()`. The crash occurs in upstream builds where `WITH_VERBOSE_WINPR_ASSERT=ON` (default in FreeRDP 3.22.0 / current WinPR CMake defaults). Smartcard redirection must be explicitly enabled by the user (e.g., `xfreerdp /smartcard`; `/smartcard-logon` implies `/smartcard`). Version 3.23.0 fixes the issue.	6.5	More Details
CVE-2026-27829	Astro is a web framework. In versions 9.0.0 through 9.5.3, a bug in Astro's image pipeline allows bypassing `image.domains` / `image.remotePatterns` restrictions, enabling the server to fetch content from unauthorized remote hosts. Astro provides an `inferSize` option that fetches remote images at render time to determine their dimensions. Remote image fetches are intended to be restricted to domains the site developer has manually authorized (using the `image.domains` or `image.remotePatterns` options). However, when `inferSize` is used, no domain validation is performed — the image is fetched from any host regardless of the configured restrictions. An attacker who can influence the image URL (e.g., via CMS content or user-supplied data) can cause the server to fetch from arbitrary hosts. This allows bypassing `image.domains` / `image.remotePatterns` restrictions to make server-side requests to unauthorized hosts. This	6.5	More Details

	includes the risk of server-side request forgery (SSRF) against internal network services and cloud metadata endpoints. Version 9.5.4 fixes the issue.		
CVE-2026-22878	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2024-43766	In multiple functions of btm_ble_sec.cc, there is a possible unencrypted communication due to Invalid error handling. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-27598	Dagu is a workflow engine with a built-in Web user interface. In versions up to and including 1.16.7, the `CreateNewDAG` API endpoint (`POST /api/v1/dags`) does not validate the DAG name before passing it to the file store. An authenticated user with DAG write permissions can write arbitrary YAML files anywhere on the filesystem (limited by the process permissions). Since dagu executes DAG files as shell commands, writing a malicious DAG to the DAGs directory of another instance or overwriting config files can lead to remote code execution. Commit e2ed589105d79273e4e6ac8eb31525f765bb3ce4 fixes the issue.	6.5	More Details
CVE-2026-26937	Uncontrolled Resource Consumption (CWE-400) in the Timelion component in Kibana can lead Denial of Service via Input Data Manipulation (CAPEC-153)	6.5	More Details
CVE-2026-27754	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 use the cryptographically broken MD5 hash function for session cookie generation, weakening session security. Attackers can exploit predictable session tokens combined with MD5's collision vulnerabilities to forge valid session cookies and gain unauthorized access to the device.	6.5	More Details
CVE-2026-25774	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2024-10938	The OVRI Payment plugin for WordPress contains malicious .htaccess files in version 1.7.0. The files contain directives to prevent the execution of certain scripts while allowing execution of known malicious PHP files. If moved outside of the plugin's directory, they may interfere with the proper function of a site.	6.5	More Details
CVE-2026-27611	FileBrowser Quantum is a free, self-hosted, web-based file manager. Prior to versions 1.1.3-stable and 1.2.6-beta, when users share password-protected files, the recipient can completely bypass the password and still download the file. This happens because the API returns a direct download link in the details of the share, which is accessible to anyone with JUST THE SHARE LINK, even without the password. Versions 1.1.3-stable and 1.2.6-beta fix the issue.	6.5	More Details
CVE-2026-1627	An attacker may exploit the use of outdated and weak MAC algorithms in the device’s SSH service to potentially compromise the integrity of the SSH session, allowing manipulation of transmitted data if the attacker can interact with the network traffic.	6.5	More Details
CVE-2026-1626	An attacker may exploit the use of weak CBC-based cipher suites in the device’s SSH service to potentially observe or manipulate parts of the encrypted SSH communication, if they are able to intercept or interact with the network traffic.	6.5	More Details
CVE-2026-27705	Plane is an an open-source project management tool. Prior to version 1.2.2, the `ProjectAssetEndpoint.patch()` method in `apps/api/plane/app/views/asset/v2.py` (lines 579–593) performs a global asset lookup using only the asset ID (`pk`) via `FileAsset.objects.get(id=pk)`, without verifying that the asset belongs to the workspace and project specified in the URL path. This allows any authenticated user (including those with the GUEST role) to modify the `attributes` and `is_uploaded` status of assets belonging to any workspace or project in the entire Plane instance by guessing or enumerating asset UUIDs. Version 1.2.2 fixes the issue.	6.5	More Details
CVE-2026-26935	Improper Input Validation (CWE-20) in the internal Content Connectors search endpoint in Kibana can lead Denial of Service via Input Data Manipulation (CAPEC-153)	6.5	More Details
CVE-2026-26934	Improper Validation of Specified Quantity in Input (CWE-1284) in Kibana can allow an authenticated attacker with view-only privileges to cause a Denial of Service via Input Data Manipulation (CAPEC-153). An attacker can send a specially crafted, malformed payload causing	6.5	More Details

	excessive resource consumption and resulting in Kibana becoming unresponsive or crashing.		
CVE-2026-1487	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to SQL Injection via the JSON Import in all versions up to, and including, 5.2.7 due to insufficient validation on the user-supplied JSON data. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute arbitrary SQL queries on the database that can be used to extract information via time-based techniques, drop tables, or modify data.	6.5	More Details
CVE-2026-25554	OpenSIPS versions 3.1 before 3.6.4 containing the auth_jwt module (prior to commit 3822d33) contain a SQL injection vulnerability in the jwt_db_authorize() function in modules/auth_jwt/authorize.c when db_mode is enabled and a SQL database backend is used. The function extracts the tag claim from a JWT without prior signature verification and incorporates the unescaped value directly into a SQL query. An attacker can supply a crafted JWT with a malicious tag claim to manipulate the query result and bypass JWT authentication, allowing impersonation of arbitrary identities.	6.5	More Details
CVE-2026-28131	Insertion of Sensitive Information Into Sent Data vulnerability in WPVibes Elementor Addon Elements addon-elements-for-elementor-page-builder allows Retrieve Embedded Sensitive Data.This issue affects Elementor Addon Elements: from n/a through <= 1.14.4.	6.5	More Details
CVE-2026-2256	A command injection vulnerability in ModelScope's ms-agent versions v1.6.0rc1 and earlier exists, allowing an attacker to execute arbitrary operating system commands through crafted prompt-derived input.	6.5	More Details
CVE-2026-25127	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the server does not properly validate user permission. Unauthorized users can view the information of authorized users. Version 8.0.0 fixes the issue.	6.5	More Details
CVE-2025-13616	IBM DataStage on Cloud Pak for Data 5.1.2 through 5.3.0 returns sensitive information in an HTTP response that could be used in further attacks against the system.	6.5	More Details
CVE-2026-25930	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the Layout-Based Form (LBF) printable view accepts `formid` and `visitid` (or `patientid`) from the request and does not verify that the form belongs to the current user's authorized patient/encounter. An authenticated user with LBF access can enumerate form IDs and view or print any patient's encounter forms. Version 8.0.0 fixes the issue.	6.5	More Details
CVE-2026-28354	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 #59, collection item operations are vulnerable to authorization flaws, allowing a normal authenticated user to modify another user's collection items. This affects both add item (/actions/add_to_collection.php) due to missing authorization checks and delete item (/manage_collections.php?mode=manage_items...) due to a broken ownership check in removeItemFromCollection(). As a result, attackers can insert and remove items from collections they do not own. Version 5.5.3 #59 fixes the issue.	6.5	More Details
CVE-2026-3255	HTTP::Session2 versions before 1.12 for Perl for Perl may generate weak session ids using the rand() function. The HTTP::Session2 session id generator returns a SHA-1 hash seeded with the built-in rand function, the epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand() function is unsuitable for cryptographic usage. HTTP::Session2 after version 1.02 will attempt to use the /dev/urandom device to generate a session id, but if the device is unavailable (for example, under Windows), then it will revert to the insecure method described above.	6.5	More Details
CVE-2018-25160	HTTP::Session2 versions through 1.09 for Perl does not validate the format of user provided session ids, enabling code injection or other impact depending on session backend. For example, if an application uses memcached for session storage, then it may be possible for a remote attacker to inject memcached commands in the session id value.	6.5	More Details
CVE-2025-47384	Transient DOS when MAC configures config id greater than supported maximum value.	6.5	More Details
CVE-2026-28271	Kiteworks is a private data network (PDN). Prior to version 9.2.0, a vulnerability in Kiteworks configuration functionality allows bypassing of SSRF protections through DNS rebinding attacks. Malicious administrators could exploit this to access internal services that should be restricted. Version 9.2.0 contains a patch for the issue.	6.5	More Details

CVE-2026-25124	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the OpenEMR application is vulnerable to an access control flaw that allows low-privileged users, such as receptionists, to export the entire message list containing sensitive patient and user data. The vulnerability lies in the message_list.php report export functionality, where there is no permission check before executing sensitive database queries. The only control in place is CSRF token verification, which does not prevent unauthorized data access if the token is acquired through other means. Version 8.0.0 fixes the vulnerability.	6.5	More Details
CVE-2026-28352	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. In versions prior to 3.3.11, the API endpoint used to manage event series is missing an access check, allowing unauthenticated/unauthorized access to this endpoint. The impact of this is limited to getting the metadata (title, category chain, start/end date) for events in an existing series, deleting an existing event series, and modifying an existing event series. This vulnerability does NOT allow unauthorized access to events (beyond the basic metadata mentioned above), nor any kind of tampering with user-visible data in events. Version 3.3.11 fixes the issue. As a workaround, use the webserver to restrict access to the series management API endpoint.	6.5	More Details
CVE-2026-27609	Parse Dashboard is a standalone dashboard for managing Parse Server apps. In versions 7.3.0-alpha.42 through 9.0.0-alpha.7, the AI Agent API endpoint (`POST /apps/:appId/agent`) lacks CSRF protection. An attacker can craft a malicious page that, when visited by an authenticated dashboard user, submits requests to the agent endpoint using the victim's session. The fix in version 9.0.0-alpha.8 adds CSRF middleware to the agent endpoint and embeds a CSRF token in the dashboard page. As a workaround, remove the `agent` configuration block from your dashboard configuration. Dashboards without an `agent` config are not affected.	6.5	More Details
CVE-2026-26077	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, several webhook endpoints (SendGrid, Mailjet, Mandrill, Postmark, SparkPost) in the `WebhooksController` accepted requests without a valid authentication token when no token was configured. This allowed unauthenticated attackers to forge webhook payloads and artificially inflate user bounce scores, potentially causing legitimate user emails to be disabled. The Mailpace endpoint had no token validation at all. Starting in versions 2025.12.2, 2026.1.1, and 2026.2.0, all webhook endpoints reject requests with a 406 response when no authentication token is configured. As a workaround, ensure that webhook authentication tokens are configured for all email provider integrations in site settings (e.g., `sendgrid_verification_key`, `mailjet_webhook_token`, `postmark_webhook_token`, `sparkpost_webhook_token`). There's no current workaround for mailpace before getting this fix.	6.5	More Details
CVE-2026-28557	wpForo Forum 2.4.14 contains a missing capability check vulnerability that allows authenticated users to trigger bulk wpForo usergroup reassignment via the wpforo_synch_roles AJAX handler. Attackers access the usergroups admin page, accessible to any authenticated user, to obtain a nonce, then remap all wpForo usergroups to arbitrary WordPress roles.	6.5	More Details
CVE-2025-3525	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.0 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have, under certain circumstances, allowed an authenticated user with certain access to cause Denial of Service by creating specially crafted CI triggers via the API.	6.5	More Details
CVE-2026-1542	The Super Stage WP WordPress plugin through 1.0.1 unserializes user input via REQUEST, which could allow unauthenticated users to perform PHP Object Injection when a suitable gadget is present on the blog.	6.5	More Details
CVE-2026-27149	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, SQL injection in PM tag filtering (`list_private_messages_tag`) allows bypassing tag filter conditions, potentially disclosing unauthorized private message metadata. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	6.5	More Details
CVE-2026-28424	Statmatic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.11 and 6.4.0, user email addresses were included in responses from the user fieldtype's data endpoint for control panel users who did not have the "view users" permission. This has been fixed in 5.73.11 and 6.4.0.	6.5	More Details
CVE-2026-28396	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, the password reset flow did not revoke existing refresh tokens, allowing an attacker with a previously stolen refresh token to continue minting valid JWTs after the victim resets their password. This issue has been patched in version 0.301.3.	6.5	More Details

CVE-2026-25929	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the document controller's `patient_picture` context serves the patient's photo by document ID or patient ID without verifying that the current user is authorized to access that patient. An authenticated user with document ACL can supply another patient's ID and retrieve their photo. Version 8.0.0 fixes the issue.	6.5	More Details
CVE-2026-24896	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, a Broken Access Control vulnerability exists in OpenEMR's edih_main.php endpoint, which allows any authenticated user—including low-privilege roles like Receptionist—to access EDI log files by manipulating the log_select parameter in a GET request. The back-end fails to enforce role-based access control (RBAC), allowing sensitive system logs to be accessed outside the GUI-enforced permission boundaries. Version 8.0.0 fixes the issue.	6.5	More Details
CVE-2026-2606	IBM webMethods API Gateway (on-prem) 10.11 through 10.11_Fix3210.15 to 10.15_Fix2711.1 to 11.1_Fix7 IBM webMethods API Management (on-prem) fails to properly validate user-supplied input passed to the url parameter on the /createapi endpoint. An attacker can modify this parameter to use a file:// URI schema instead of the expected https:// schema, enabling unauthorized arbitrary file read access on the underlying server file system.	6.5	More Details
CVE-2025-47371	Transient DOS when an LTE RLC packet with invalid TB is received by UE.	6.5	More Details
CVE-2026-20733	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2024-55019	Incorrect access control in the component download_wb.cgi of Weintek cMT-3072XH2 easyweb Web Version v2.1.53, OS v20231011 allows unauthenticated attack to download arbitrary files.	6.5	More Details
CVE-2026-24487	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, an authorization bypass vulnerability in the FHIR CareTeam resource endpoint allows patient-scoped FHIR tokens to access care team data for all patients instead of being restricted to only the authenticated patient's data. This could potentially lead to unauthorized disclosure of Protected Health Information (PHI), including patient-provider relationships and care team structures across the entire system. The issue occurs because the `FhirCareTeamService` does not implement the `IPatientCompartmentResourceService` interface and does not pass the patient binding parameter to the underlying service, bypassing the patient compartment filtering mechanism. Version 8.0.0 contains a patch for this issue.	6.5	More Details
CVE-2026-27734	Beszel is a server monitoring platform. Prior to version 0.18.2, the hub's authenticated API endpoints GET /api/beszel/containers/logs and GET /api/beszel/containers/info pass the user-supplied "container" query parameter to the agent without validation. The agent constructs Docker Engine API URLs using fmt.Sprintf with the raw value instead of url.PathEscape(). Since Go's http.Client does not sanitize `../` sequences from URL paths sent over unix sockets, an authenticated user (including readonly role) can traverse to arbitrary Docker API endpoints on agent hosts, exposing sensitive infrastructure details. Version 0.18.4 fixes the issue.	6.5	More Details
CVE-2026-20036	A vulnerability in the CLI and web-based management interface of Cisco UCS Manager Software could allow an authenticated, remote attacker with valid administrative privileges to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation of command arguments that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of an affected device with root-level privileges.	6.5	More Details
CVE-2026-27793	Seerr is an open-source media request and discovery manager for Jellyfin, Plex, and Emby. Prior to version 3.1.0, the `GET /api/v1/user/:id` endpoint returns the full settings object for any user, including Pushover, Pushbullet, and Telegram credentials, to any authenticated requester regardless of their privilege level. This vulnerability can be exploited alone or combined with the reported unauthenticated account creation vulnerability, CVE-2026-27707. When combined, the two vulnerabilities create a zero-prior-access chain that leaks third-party API credentials for all users, including administrators. Version 3.1.0 contains a fix for both this vulnerability and for CVE-	6.5	More Details

	2026-27707.		
CVE-2026-20791	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-25963	Fleet is open source device management software. In versions prior to 4.80.1, a broken authorization check in Fleet's certificate template deletion API could allow a team administrator to delete certificate templates belonging to other teams within the same Fleet instance. Fleet supports certificate templates that are scoped to individual teams. In affected versions, the batch deletion endpoint validated authorization using a user-supplied team identifier but did not verify that the certificate template IDs being deleted actually belonged to that team. As a result, a team administrator could delete certificate templates associated with other teams, potentially disrupting certificate-based workflows such as device enrollment, Wi-Fi authentication, VPN access, or other certificate-dependent configurations for the affected teams. This issue does not allow privilege escalation, access to sensitive data, or compromise of Fleet's control plane. Impact is limited to integrity and availability of certificate templates across teams. Version 4.80.1 patches the issue. If an immediate upgrade is not possible, administrators should restrict access to certificate template management to trusted users and avoid delegating team administrator permissions where not strictly required.	6.5	More Details
CVE-2026-3100	The FTP Backup on the ADM will not properly strictly enforce TLS certificate verification while connecting to an FTP server using FTPES/FTPS. An improper validated TLS/SSL certificates allows a remote attacker can intercept network traffic to perform a Man-in-the-Middle (MitM) attack, which may intercept, modify, or obtain sensitive information such as authentication credentials and backup data. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.2.RE51.	6.5	More Details
CVE-2026-27465	Fleet is open source device management software. In versions prior to 4.80.1, a vulnerability in Fleet's configuration API could expose Google Calendar service account credentials to authenticated users with low-privilege roles. This may allow unauthorized access to Google Calendar resources associated with the service account. Fleet returns configuration data through an API endpoint that is accessible to authenticated users, including those with the lowest-privilege "Observer" role. In affected versions, Google Calendar service account credentials were not properly obfuscated before being returned. As a result, a low-privilege user could retrieve the service account's private key material. Depending on how the Google Calendar integration is configured, this could allow unauthorized access to calendar data or other Google Workspace resources associated with the service account. This issue does not allow escalation of privileges within Fleet or access to device management functionality. Version 4.80.1 patches the issue. If an immediate upgrade is not possible, administrators should remove the Google Calendar integration from Fleet and rotate the affected Google service account credentials.	6.5	More Details
CVE-2026-28412	Textream is a free macOS teleprompter app. Prior to version 1.5.1, the `DirectorServer` WebSocket server imposes no limit on concurrent connections. Combined with a broadcast timer that sends state to all connected clients every 100 ms, an attacker can exhaust CPU and memory by flooding the server with connections, causing the Textream application to freeze and crash during a live session. Version 1.5.1 fixes the issue.	6.5	More Details
CVE-2026-22890	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-25220	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the Message Center accepts the URL parameter `show_all=yes` and passes it to `getPnotesByUser()`, which returns all internal messages (all users' notes). The backend does not verify that the requesting user is an administrator before honoring `show_all=yes`. The "Show All" link is also visible to non-admin users. As a result, any authenticated user can view the entire internal message list by requesting `messages.php?show_all=yes`. Version 8.0.0 patches the issue.	6.5	More Details
CVE-2026-28226	Phishing Club is a phishing simulation and man-in-the-middle framework. Prior to version 1.30.2, an authenticated SQL injection vulnerability exists in the GetOrphaned recipient listing endpoint in versions prior to v1.30.2. The endpoint constructs a raw SQL query and concatenates the user-controlled sortBy value directly into the ORDER BY clause without allowlist validation. Because unknown values are silently passed through `RemapOrderBy()`, an authenticated attacker can inject SQL expressions into the `ORDER BY` clause. This issue was patched in v1.30.2 by	6.5	More Details

	validating the order-by column against an allowlist and clearing unknown mappings.		
CVE-2026-28217	hoppscotch is an open source API development ecosystem. Prior to version 2026.2.0, the `userCollection` GraphQL query accepts an arbitrary collection ID and returns the full collection data — including title, type, and the serialized `data` field containing HTTP requests with headers and potentially secrets — to any authenticated user, without verifying that the requesting user owns the collection. This is an Insecure Direct Object Reference (IDOR) caused by a missing authorization check that exists on every other operation in the same resolver. Version 2026.2.0 fixes the issue.	6.5	More Details
CVE-2024-55025	Incorrect access control in the VNC component of Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 allows unauthorized attackers to access the HMI system.	6.5	More Details
CVE-2025-14040	The Automotive Car Dealership Business WordPress Theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Call to Action' custom fields in all versions up to, and including, 13.4. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the 'action_text', 'action_button_text', 'action_link', and 'action_class' custom fields. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14142	The Electric Enquiries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button' parameter of the electric-enquiry shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2026-28558	wpForo Forum 2.4.14 contains a stored cross-site scripting vulnerability that allows authenticated subscribers to upload SVG files as profile avatars through the avatar upload functionality. Attackers upload a crafted SVG containing CSS injection or JavaScript event handlers that execute in the browsers of any user who views the attacker's profile page.	6.4	More Details
CVE-2026-20438	In MAE, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10431920; Issue ID: MSV-5835.	6.4	More Details
CVE-2026-27810	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Prior to version 9.4.0, an HTTP Response Header Injection vulnerability in the calibre Content Server allows any authenticated user to inject arbitrary HTTP headers into server responses via an unsanitized `content_disposition` query parameter in the `/get/` and `/data-files/get/` endpoints. All users running the calibre Content Server with authentication enabled are affected. The vulnerability is exploitable by any authenticated user and can also be triggered by tricking an authenticated victim into clicking a crafted link. Version 9.4.0 contains a fix for the issue.	6.4	More Details
CVE-2026-2362	The WP Accessibility plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'alt' attribute of images processed by the "Long Description UI" feature in all versions up to, and including, 2.3.1. This is due to the plugin's JavaScript retrieving the alt attribute using getAttribute() and unsafely concatenating it into innerHTML and insertAdjacentHTML calls without proper sanitization or escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the "Long Description UI" setting to be enabled and set to "Link to description."	6.4	More Details
CVE-2026-2383	The Simple Download Monitor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom field in all versions up to, and including, 4.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2367	The Secure Copy Content Protection and Content Locking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ays_block' shortcode in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-14149	The Xpro Addons — 140+ Widgets for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Scroller widget box link attribute in all versions up to, and including, 1.4.24 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-2026-2583	The Blocksy theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `blocksy_meta` metadata fields in all versions up to, and including, 2.1.30 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-2026-1614	The Rise Blocks – A Complete Gutenberg Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'logoTag' Site Identity block attribute in all versions up to, and including, 3.7 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-2026-2029	The Livemesh Addons for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `[labb_pricing_item]` shortcode's `title` and `value` attributes in all versions up to, and including, 3.9.2 due to insufficient input sanitization and output escaping. Specifically, the plugin uses `htmlspecialchars_decode()` after `wp_kses_post()`, which decodes HTML entities back into executable code after sanitization has occurred. 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-2026-3149	A weakness has been identified in itsourcecode College Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/asign-single-student-subjects.php. Executing a manipulation of the argument course_code can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-27837	Dottie provides nested object access and manipulation in JavaScript. Versions 2.0.4 through 2.0.6 contain an incomplete fix for CVE-2023-26132. The prototype pollution guard introduced in commit `7d3aee1` only validates the first segment of a dot-separated path, allowing an attacker to bypass the protection by placing `__proto__` at any position other than the first. Both `dottie.set()` and `dottie.transform()` are affected. Version 2.0.7 contains an updated fix to address the residual vulnerability.	6.3	More Details
CVE-2025-11950	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in KNOWHY Advanced Technology Trading Ltd. Co. EduAsist allows Reflected XSS.This issue affects EduAsist: through 27022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3262	A vulnerability has been found in go2ismail Asp.Net-Core-Inventory-Order-Management-System up to 9.20250118. Affected is an unknown function of the component Administrative Interface. Such manipulation leads to execution after redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3187	A vulnerability was identified in feiyuchuixue sz-boot-parent up to 1.3.2-beta. Affected by this issue is some unknown functionality of the file /api/admin/sys-file/upload of the component API Endpoint. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit is publicly available and might be used. Upgrading to version 1.3.3-beta can resolve this issue. The name of the patch is aefaabfd7527188bfba3c8c9eee17c316d094802. Upgrading the affected component is recommended. The project was informed beforehand and acted very professional: "We have introduced a whitelist restriction on the /api/admin/sys-file/upload endpoint via the oss.allowedExts and oss.allowedMimeTypes configuration options, allowing the specification of permitted file extensions and MIME types for uploads."	6.3	More Details
CVE-2026-3263	A vulnerability was found in go2ismail Asp.Net-Core-Inventory-Order-Management-System up to 9.20250118. Affected by this vulnerability is an unknown functionality of the file /api/Security/ of the component Security API. Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2026-3163	A vulnerability has been found in SourceCodester Website Link Extractor 1.0. This vulnerability affects the function file_get_contents of the component URL Handler. The manipulation leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-13687	IBM DataStage on Cloud Pak for Data 5.1.2 through 5.3.0 could allow an authenticated user to execute arbitrary commands with normal user privileges on the system due to improper validation of user supplied input through the user-defined function component.	6.3	More Details
CVE-2026-3270	A vulnerability has been found in psi-probe PSI Probe up to 5.3.0. This affects the function lookup of the file psi-probe-core/src/main/java/psiprobe/tools/Whois.java of the component Whois. The manipulation leads to server-side request forgery. 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.	6.3	More Details
CVE-2026-28230	SteVe is an open-source EV charging station management system. In versions up to and including 3.11.0, when a charger sends a StopTransaction message, SteVe looks up the transaction solely by transactionId (a sequential integer starting from 1) without verifying that the requesting charger matches the charger that originally started the transaction. Any authenticated charger can terminate any other charger's active session across the entire network. The root cause is in OcppServerRepositoryImpl.getTransaction() which queries only by transactionId with no chargeBoxId ownership check. The validator checks that the transaction exists and is not already stopped but never verifies identity. As an attacker controlling a single registered charger I could enumerate sequential transaction IDs and send StopTransaction messages targeting active sessions on every other charger on the network simultaneously. Combined with FINDING-014 (unauthenticated SOAP endpoints), no registered charger is even required — the attack is executable with a single curl command requiring only a known chargeBoxId. Commit 7f169c6c5b36a9c458ec41ce8af581972e5c724e contains a fix for the issue.	6.3	More Details
CVE-2025-15597	A vulnerability has been found in Dataease SQLBot up to 1.4.0. This affects an unknown function of the file backend/apps/system/api/assistant.py of the component API Endpoint. Such manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.0 mitigates this issue. The name of the patch is d640ac31d1ce64ce90e06cf7081163915c9fc28c. Upgrading the affected component is recommended. Multiple endpoints are affected. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-3286	A vulnerability was identified in itwanger paicoding 1.0.0/1.0.1/1.0.2/1.0.3. The impacted element is the function Save of the file paicoding-web/src/main/java/com/github/paicoding/forum/web/common/image/rest/ImageRestController.java of the component Image Save Endpoint. Such manipulation of the argument img leads to server-side request forgery. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3264	A vulnerability was determined in go2ismail Free-CRM up to b83c40a90726d5e58f0cc680ffdcaa28a03fb5d1. Affected by this issue is some unknown functionality of the component Administrative Interface. Executing a manipulation can lead to execution after redirect. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3265	A vulnerability was identified in go2ismail Free-CRM up to b83c40a90726d5e58f0cc680ffdcaa28a03fb5d1. This affects an unknown part of the file /api/Security/ of the component Security API. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13688	IBM DataStage on Cloud Pak for Data 5.1.2 through 5.3.0 could allow an authenticated user to execute arbitrary commands with normal user privileges on the system due to improper validation of user supplied input through the wrapped command component.	6.3	More Details

CVE-2026-3150	A security vulnerability has been detected in itsourcecode College Management System 1.0. This affects an unknown part of the file /admin/display-teacher.php. The manipulation of the argument teacher_id leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-13686	IBM DataStage on Cloud Pak for Data 5.1.2 through 5.3.0 could allow an authenticated user to execute arbitrary commands with normal user privileges on the system due to improper validation of user supplied input through the job subroutine component.	6.3	More Details
CVE-2026-28361	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, the MCP token service did not validate token ownership, allowing a Creator within the same base to read, regenerate, or delete another user's MCP tokens if the token ID was known. This issue has been patched in version 0.301.3.	6.3	More Details
CVE-2026-3484	A vulnerability was detected in PhialsBasement nmap-mcp-server up to bee6d23547d57ae02460022f7c78ac0893092e38. Affected by this issue is the function child_process.exec of the file src/index.ts of the component Nmap CLI Command Handler. The manipulation results in command injection. The attack may be performed from remote. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The patch is identified as 30a6b9e1c7fa6146f51e28d6ab83a2568d9a3488. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-3287	A security flaw has been discovered in youlaitech youlai-mall 2.0.0. This affects the function listPagedSpuForApp of the file mall-pms/pms-boot/src/main/java/com/youlai/mall/pms/controller/app/SpuController.java of the component App-side Product Pagination Endpoint. Performing a manipulation of the argument sortField/sort results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3289	A weakness has been identified in Sanluan PublicCMS 6.202506.d. This impacts the function saveMetadata of the file TemplateCacheComponent.java of the component Template Cache Generation. Executing a manipulation can lead to path traversal. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3292	A security vulnerability has been detected in jizhiCMS up to 2.5.6. Affected is the function findAll in the library frphp/lib/Model.php of the component Batch Interface. The manipulation of the argument data leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3186	A vulnerability was determined in feiyuchuixue sz-boot-parent up to 1.3.2-beta. Affected by this vulnerability is an unknown functionality of the file /api/admin/sys-user/reset/password/ of the component Password Reset Handler. This manipulation of the argument userId causes use of default password. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.3.3-beta addresses this issue. Patch name: aefaabfd7527188bfba3c8c9eee17c316d094802. It is suggested to upgrade the affected component. The project was informed beforehand and acted very professional: "We have added authorization validation to the password reset interface; now only users with the corresponding permissions are allowed to perform password resets."	6.3	More Details
CVE-2026-3209	A vulnerability has been found in fosrl Pangolin up to 1.15.4-s.3. This affects the function verifyRoleAccess/verifyApiKeyRoleAccess of the component Role Handler. The manipulation leads to improper access controls. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. Upgrading to version 1.15.4-s.4 mitigates this issue. The identifier of the patch is 5e37c4e85fae68e756be5019a28ca903b161fdd5. Upgrading the affected component is advised.	6.3	More Details
CVE-2025-13327	A flaw was found in uv. This vulnerability allows an attacker to execute malicious code during package resolution or installation via specially crafted ZIP (Zipped Information Package) archives that exploit parsing differentials, requiring user interaction to install an attacker-controlled package.	6.3	More Details
CVE-	In multiple functions of ProfilingService.java, there is a possible persistent denial of service due to		More

2025-48587	improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	Details
CVE-2025-48585	In multiple functions of ProfilingService.java, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2025-36364	IBM DevOps Plan 3.0.0 through 3.0.5 allows web page cache to be stored locally which can be read by another user on the system.	6.2	More Details
CVE-2026-0005	In onServiceDisconnected of KeyguardServiceDelegate.java, there is a possible partial bypass of app pinning allowing limited interaction with other apps without knowing the LSKF due to a missing permission check. This could lead to local information disclosure where the extent of interaction and impact is app-dependent with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-0012	In setHideSensitive of ExpandableNotificationRow.java, there is a possible contact name leak due due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-0014	In isPackageNullOrSystem of AppOpsService.java, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-22721	VMware Aria Operations contains a privilege escalation vulnerability. A malicious actor with privileges in vCenter to access Aria Operations may leverage this vulnerability to obtain administrative access in VMware Aria Operations. To remediate CVE-2026-22721, apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' found in VMSA-2026-0001 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947 .	6.2	More Details
CVE-2026-27846	Due to missing authentication, a user with physical access to the device can misuse the mesh functionality for adding a new mesh device to the network to gain access to sensitive information, including the password for admin access to the web interface and the Wi-Fi passwords.This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	6.2	More Details
CVE-2026-0015	In multiple locations of AppOpsService.java, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-27691	iccDEV provides a set of libraries and tools for working with ICC color management profiles. In versions up to and including 2.3.1.4, signed integer overflow in iccFromCube.cpp during multiplication triggers undefined behavior, potentially causing crashes or incorrect ICC profile generation when processing crafted/large cube inputs. Commit 43ae18dd69fc70190d3632a18a3af2f3da1e052a fixes the issue. No known workarounds are available.	6.2	More Details
CVE-2026-2680	Reflected Cross-Site Scripting (XSS) on the A3factura web platform, in parameter 'customerVATNumber', in 'a3factura-app.wolterskluwer.es/#/incomes/salesDeliveryNotes' endpoint, which could allow an attacker to execute arbitrary code in the victim's browser.	6.1	More Details
CVE-2026-27154	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, a user full name can be evaluated as raw HTML when the following settings are set: `display_name_on_posts` => true; and `prioritize_username_in_ux` => false. Editing a post of a malicious user would trigger an XSS. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	6.1	More Details
CVE-2026-27746	The SPIP jeux plugin versions prior to 4.1.1 contain a reflected cross-site scripting (XSS) vulnerability in the pre_propre pipeline. The plugin incorporates untrusted request parameters into HTML output without proper output encoding, allowing attackers to inject arbitrary script content into pages that render a jeux block. When a victim is induced to visit a crafted URL, the injected content is reflected into the response and executed in the victim's browser context.	6.1	More Details
CVE-2026-	Reflected Cross-Site Scripting (XSS) on the A3factura web platform, in parameter 'customerName', in 'a3factura-app.wolterskluwer.es/#/incomes/salesInvoices' endpoint, which	6.1	More Details

2679	could allow an attacker to execute arbitrary code in the victim's browser.		
CVE-2025-15599	DOMPurify 3.1.3 through 3.2.6 and 2.5.3 through 2.5.8 contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting missing textarea rawtext element validation in the SAFE_FOR_XML regex. Attackers can include closing rawtext tags like </textarea> in attribute values to break out of rawtext contexts and execute JavaScript when sanitized output is placed inside rawtext elements. The 3.x branch was fixed in 3.2.7; the 2.x branch was never patched.	6.1	More Details
CVE-2025-65465	A reflected Cross-Site Scripting (XSS) vulnerability in the RaiseError function of Skrol29 TbsZip version 2.17 and earlier allows remote attackers to execute arbitrary web script or HTML via a crafted payload in a filename parameter (e.g., to the FileRead function). This occurs because the error message is not properly sanitized before being output to the user. This vulnerability is fixed in version 2.18.	6.1	More Details
CVE-2026-27756	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a reflected cross-site scripting vulnerability in the management interface where user input is not properly encoded before output. Attackers can craft malicious URLs that execute arbitrary JavaScript in the web interface when visited by authenticated users.	6.1	More Details
CVE-2025-66880	Cross Site Scripting vulnerability in Wethink Technology Inc 720yun pano-sdk 0.5.877 allows a remote attacker to execute arbitrary code via the LoginComp (Module 2093) and SignupComp (Module 2094) modules.	6.1	More Details
CVE-2026-27970	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Versions prior to 21.2.0, 21.1.16, 20.3.17, and 19.2.19 have a cross-Site scripting vulnerability in the Angular internationalization (i18n) pipeline. In ICU messages (International Components for Unicode), HTML from translated content was not properly sanitized and could execute arbitrary JavaScript. Angular i18n typically involves three steps, extracting all messages from an application in the source language, sending the messages to be translated, and then merging their translations back into the final source code. Translations are frequently handled by contracts with specific partner companies, and involve sending the source messages to a separate contractor before receiving final translations for display to the end user. If the returned translations have malicious content, it could be rendered into the application and execute arbitrary JavaScript. When successfully exploited, this vulnerability allows for execution of attacker controlled JavaScript in the application origin. Depending on the nature of the application being exploited this could lead to credential exfiltration and/or page vandalism. Several preconditions apply to the attack. The attacker must compromise the translation file (xliff, xtb, etc.). Unlike most XSS vulnerabilities, this issue is not exploitable by arbitrary users. An attacker must first compromise an application's translation file before they can escalate privileges into the Angular application client. The victim application must use Angular i18n, use one or more ICU messages, render an ICU message, and not defend against XSS via a safe content security policy. Versions 21.2.0, 21.1.6, 20.3.17, and 19.2.19 patch the issue. Until the patch is applied, developers should consider reviewing and verifying translated content received from untrusted third parties before incorporating it in an Angular application, enabling strict CSP controls to block unauthorized JavaScript from executing on the page, and enabling Trusted Types to enforce proper HTML sanitization.	6.1	More Details
CVE-2025-52564	Chamilo is a learning management system. Prior to version 1.11.30, the open parameter of help.php fails to properly sanitize user input. This allows an attacker to inject arbitrary HTML, such as underlined text, via a crafted URL. This issue has been patched in version 1.11.30.	6.1	More Details
CVE-2026-3455	Versions of the package mailparser before 3.9.3 are vulnerable to Cross-site Scripting (XSS) via the textToHtml() function due to the improper sanitisation of URLs in the email content. An attacker can execute arbitrary scripts in victim browsers by adding extra quote " to the URL with embedded malicious JavaScript code.	6.1	More Details
CVE-2026-24847	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the Eye Exam form module allows any authenticated user to be redirected to an arbitrary external URL. This can be exploited for phishing attacks against healthcare providers using OpenEMR. Version 8.0.0 fixes the issue.	6.1	More Details
	osctrl is an osquery management solution. Prior to version 0.5.0, a stored cross-site scripting (XSS) vulnerability exists in the `osctrl-admin` on-demand query list. A user with query-level permissions can inject arbitrary JavaScript via the query parameter when running an on-demand query. The payload is stored and executes in the browser of any user (including administrators)		

CVE-2026-28280	who visits the query list page. This can be chained with CSRF token extraction to escalate privileges and take actions as the logged in user. An attacker with query-level permissions (the lowest privilege tier) can execute arbitrary JavaScript in the browsers of all users who view the query list. Depending on their level of access, it can lead to full platform compromise if an administrator executes the payload. The issue is fixed in osctrl `v0.5.0`. As a workaround, restrict query-level permissions to trusted users, monitor query list for suspicious payloads, and/or review osctrl user accounts for unauthorized administrators.	6.1	More Details
CVE-2025-52563	Chamilo is a learning management system. Prior to version 1.11.30, there is a reflected cross-site scripting (XSS) vulnerability due to insufficient sanitization of the page parameter in the session/add_users_to_session.php endpoint. This issue has been patched in version 1.11.30.	6.1	More Details
CVE-2026-25734	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the RSE metadata of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	6.1	More Details
CVE-2026-25735	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Identity Name of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	6.1	More Details
CVE-2026-27116	Vikunja is an open-source self-hosted task management platform. Prior to version 2.0.0, a reflected HTML injection vulnerability exists in the Projects module where the `filter` URL parameter is rendered into the DOM without output encoding when the user clicks "Filter." While `<script>` and `<iframe>` are blocked, `<svg>`, `<a>`, and formatting tags (`<h1>`, `<b>`, `<u>`) render without restriction — enabling SVG-based phishing buttons, external redirect links, and content spoofing within the trusted application origin. Version 2.0.0 fixes this issue.	6.1	More Details
CVE-2026-1434	Omega-PSIR is vulnerable to Reflected XSS via the lang parameter. An attacker can craft a malicious URL that, when opened, causes arbitrary JavaScript to execute in the victim’s browser. This issue was fixed in 4.6.7.	6.1	More Details
CVE-2026-21443	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, the `xl()` translation function returns unescaped strings. While wrapper functions exist for escaping in different contexts (`xlt()` for HTML, `xla()` for attributes, `xlj()` for JavaScript), there are places in the codebase where `xl()` output is used directly without escaping. If an attacker could insert malicious content into the translation database, these unescaped outputs could lead to XSS. Version 8.0.0 fixes the issue.	6.1	More Details
CVE-2026-27612	Repostat is a React component to fetch and display GitHub repository info. Prior to version 1.0.1, the `RepoCard` component is vulnerable to Reflected Cross-Site Scripting (XSS). The vulnerability occurs because the component uses React's `dangerouslySetInnerHTML` to render the repository name (`repo` prop) during the loading state without any sanitization. If a developer using this package passes unvalidated user input directly into the `repo` prop (for example, reading it from a URL query parameter), an attacker can execute arbitrary JavaScript in the context of the user's browser. In version 1.0.1, the use of dangerouslySetInnerHTML has been removed, and the repo prop is now safely rendered using standard React JSX data binding, which automatically escapes HTML entities.	6.1	More Details
CVE-2026-2506	The EM Cost Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.3.1. This is due to the plugin storing attacker-controlled 'customer_name' data and rendering it in the admin customer list without output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the EMCC Customers page.	6.1	More Details
CVE-2026-	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Custom RSE Attribute of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI	6.1	More Details

25736	without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.		
CVE-2026-2677	Reflected Cross-Site Scripting (XSS) on the A3factura web platform, in parameter 'name', in 'a3factura-app.wolterskluwer.es/#/incomes/representatives-management' endpoint, which could allow an attacker to execute arbitrary code in the victim's browser.	6.1	More Details
CVE-2026-27645	changedetection.io is a free open source web page change detection tool. In versions prior to 0.54.1, the RSS single-watch endpoint reflects the UUID path parameter directly in the HTTP response body without HTML escaping. Since Flask returns text/html by default for plain string responses, the browser parses and executes injected JavaScript. Version 0.54.1 contains a fix for the issue.	6.1	More Details
CVE-2025-52475	Chamilo is a learning management system. Prior to version 1.11.30, there is a reflected cross-site scripting (XSS) vulnerability in the admin/user_list.php endpoint. The keyword_inactive parameter is not properly sanitized, allowing attackers to inject malicious JavaScript through a crafted URL. This issue has been patched in version 1.11.30.	6.1	More Details
CVE-2026-27736	BigBlueButton is an open-source virtual classroom. In versions on the 3.x branch prior to 3.0.20, the string received with errorRedirectUrl lacks validation, using it directly in the respondWithRedirect function leads to an Open Redirect vulnerability. BigBlueButton 3.0.20 patches the issue. No known workarounds are available.	6.1	More Details
CVE-2025-64736	An out-of-bounds read vulnerability exists in the ABF parsing functionality of The Biosig Project libbiosig 3.9.2 and Master Branch (5462afb0). A specially crafted .abf file can lead to an information leak. An attacker can provide a malicious file to trigger this vulnerability.	6.1	More Details
CVE-2026-22722	A malicious actor with authenticated user privileges on a Windows based Workstation host may be able to cause a null pointer dereference error. To Remediate CVE-2026-22722, apply the patches listed in the "Fixed version" column of the 'Response Matrix'	6.1	More Details
CVE-2026-0540	DOMPurify 3.1.3 through 3.3.1 and 2.5.3 through 2.5.8, fixed in commit 729097f, contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting five missing rawtext elements (noscript, xmp, noembed, noframes, iframe) in the SAFE_FOR_XML regex. Attackers can include payloads like </noscript><img src=x onerror=alert(1)> in attribute values to execute JavaScript when sanitized output is placed inside these unprotected rawtext contexts.	6.1	More Details
CVE-2025-52476	Chamilo is a learning management system. Prior to version 1.11.30, there is a reflected cross-site scripting (XSS) vulnerability due to improper sanitization of the keyword_active parameter in admin/user_list.php. This issue has been patched in version 1.11.30.	6.1	More Details
CVE-2026-2678	Reflected Cross-Site Scripting (XSS) on the A3factura web platform, in parameter 'name', parameter 'name', in 'a3factura-app.wolterskluwer.es/#/incomes/customers' endpoint, which could allow an attacker to execute arbitrary code in the victim's browser.	6.1	More Details
CVE-2026-28208	Junrar is an open source java RAR archive library. Prior to version 7.5.8, a backslash path traversal vulnerability in `LocalFolderExtractor` allows an attacker to write arbitrary files with attacker-controlled content anywhere on the filesystem when a crafted RAR archive is extracted on Linux/Unix. This can often lead to remote code execution (e.g., overwriting shell profiles, source code, cron jobs, etc). Version 7.5.8 has a fix for the issue.	5.9	More Details
CVE-2026-28269	Kiteworks is a private data network (PDN). Prior to version 9.2.0, avulnerability in Kiteworks command execution functionality allows authenticated users to redirect command output to arbitrary file locations. This could be exploited to overwrite critical system files and gain elevated access. Version 9.2.0 contains a patch.	5.9	More Details
CVE-2026-27752	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 transmit authentication credentials over unencrypted HTTP, allowing attackers to capture credentials. An attacker positioned to observe network traffic between a user and the device can intercept credentials and reuse them to gain administrative access to the gateway.	5.9	More Details
CVE-2025-	IBM App Connect Operator versions CD 11.3.0 through 11.6.0 and 12.1.0 through 12.20.0, LTS versions 12.0.0 through 12.0.20, and IBM App Connect Enterprise Certified Containers Operands versions CD 12.0.11.2-r1 through 12.0.12.5-r1 and 13.0.1.0-r1 through 13.0.6.1-r1, and LTS versions 12.0.12-r1 through 12.0.12-r20, contain a vulnerability in which the IBM App Connect	5.9	More Details

13490	Enterprise Certified Container transmits data in clear text, potentially allowing an attacker to intercept and obtain sensitive information through man-in-the-middle techniques.		
CVE-2025-14456	IBM MQ Appliance 9.4 CD through 9.4.4.0 to 9.4.4.1	5.9	More Details
CVE-2026-27629	InvenTree is an Open Source Inventory Management System. Prior to version 1.2.3, insecure server-side templates can be hijacked to expose secure information to the client. When generating custom batch codes, the InvenTree server makes use of a customizable jinja2 template, which can be modified by a staff user to exfiltrate sensitive information or perform code execution on the server. This issue requires access by a user with granted staff permissions, followed by a request to generate a custom batch code via the API. Once the template has been modified in a malicious manner, the API call to generate a new batch code could be made by other users, and the template code will be executed with their user context. The code has been patched to ensure that all template generation is performed within a secure sandboxed context. This issue has been addressed in version 1.2.3, and any versions from 1.3.0 onwards. Some workarounds are available. The batch code template is a configurable global setting which can be adjusted via any user with staff access. To prevent this setting from being edited, it can be overridden at a system level to a default value, preventing it from being edited. This requires system administrator access, and cannot be changed from the client side once the server is running. It is recommended that for InvenTree installations prior to 1.2.3 the `STOCK_BATCH_CODE_TEMPLATE` and `PART_NAME_FORMAT` global settings are overridden at the system level to prevent editing.	5.9	More Details
CVE-2025-36363	IBM DevOps Plan 3.0.0 through 3.0.5 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	5.9	More Details
CVE-2026-3337	Observable timing discrepancy in AES-CCM decryption in AWS-LC allows an unauthenticated user to potentially determine authentication tag validity via timing analysis. The impacted implementations are through the EVP CIPHER API: EVP_aes_128_ccm, EVP_aes_192_ccm, and EVP_aes_256_ccm. Customers of AWS services do not need to take action. Applications using AWS-LC should upgrade to AWS-LC version 1.69.0.	5.9	More Details
CVE-2026-22715	VMWare Workstation and Fusion contain a logic flaw in the management of network packets. Known attack vectors: A malicious actor with administrative privileges on a Guest VM may be able to interrupt or intercept network connections of other Guest VM's. Resolution: To remediate CVE-2026-22715 please upgrade to VMware Workstation or Fusion Version 25H2U1	5.9	More Details
CVE-2026-27808	Mailpit is an email testing tool and API for developers. Prior to version 1.29.2, the Link Check API (/api/v1/message/{ID}/link-check) is vulnerable to Server-Side Request Forgery (SSRF). The server performs HTTP HEAD requests to every URL found in an email without validating target hosts or filtering private/internal IP addresses. The response returns status codes and status text per link, making this a non-blind SSRF. In the default configuration (no authentication on SMTP or API), this is fully exploitable remotely with zero user interaction. This is the same class of vulnerability that was fixed in the HTML Check API (CVE-2026-23845 / GHSA-6jxm-fv7w-rw5j) and the screenshot proxy (CVE-2026-21859 / GHSA-8v65-47jx-7mfr), but the Link Check code path was not included in either fix. Version 1.29.2 fixes this vulnerability.	5.8	More Details
CVE-2026-26932	Improper Validation of Array Index (CWE-129) in the PostgreSQL protocol parser in Packetbeat can lead Denial of Service via Input Data Manipulation (CAPEC-153). An attacker can send a specially crafted packet causing a Go runtime panic that terminates the Packetbeat process. This vulnerability requires the pgsql protocol to be explicitly enabled and configured to monitor traffic on the targeted port.	5.7	More Details
CVE-2025-47147	Cleartext Storage of Sensitive Information (CWE-312) in the Command Centre Mobile Client on Android and iOS could allow an attacker with access to a logged-in Operator's mobile device to extract the session token and exploit access for a limited duration. This issue affects Command Centre Mobile Client versions prior to 9.40.123.	5.7	More Details
CVE-2026-3192	A security vulnerability has been detected in Chia Blockchain 2.1.0. This issue affects the function _authenticate of the file rpc_server_base.py of the component RPC Credential Handler. The manipulation leads to improper authentication. The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit has been disclosed publicly and may be used. The vendor was informed early via email. A	5.6	More Details

	separate report via bugbounty was rejected with the reason "This is by design. The user is responsible for host security".		
CVE-2026-20801	Cleartext Transmission of Sensitive Information (CWE-319) in a component used in the Gallagher Hanwha VMS and Gallagher NxWitness VMS integrations allows unprivileged users with local network access to view live video streams. This issue affects all versions of Gallagher NxWitness VMS integration prior to 9.10.017 and Gallagher Hanwha VMS integration prior to 9.10.025.	5.6	More Details
CVE-2026-1713	IBM MQ 9.1.0.0 through 9.1.0.33 LTS, 9.2.0.0 through 9.2.0.40 LTS, 9.3.0.0 through 9.3.0.36 LTS, 9.30.0 through 9.3.5.1 CD, 9.4.0.0 through 9.4.0.17 LTS, and 9.4.0.0 through 9.4.4.1 CD	5.5	More Details
CVE-2026-2636	This vulnerability is caused by a CWE-159: "Improper Handling of Invalid Use of Special Elements" weakness, which leads to an unrecoverable inconsistency in the CLFS.sys driver. This condition forces a call to the KeBugCheckEx function, allowing an unprivileged user to trigger a system crash. Microsoft silently fixed this vulnerability in the September 2025 cumulative update for Windows 11 2024 LTSC and Windows Server 2025. Windows 25H2 (released in September) was released with the patch. Windows 1123h2 and earlier versions remain vulnerable.	5.5	More Details
CVE-2026-28561	wpForo Forum 2.4.14 contains a stored cross-site scripting vulnerability that allows administrators to inject persistent JavaScript via forum description fields echoed without output escaping across multiple theme template files. On multisite installations or with a compromised admin account, attackers set a forum description containing HTML event handlers that execute when any user views the forum listing.	5.5	More Details
CVE-2025-48644	In multiple locations, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-26104	A flaw was found in the udisks storage management daemon that allows unprivileged users to back up LUKS encryption headers without authorization. The issue occurs because a privileged D-Bus method responsible for exporting encryption metadata does not perform a policy check. As a result, sensitive cryptographic metadata can be read and written to attacker-controlled locations. This weakens the confidentiality guarantees of encrypted storage volumes.	5.5	More Details
CVE-2026-3203	RF4CE Profile protocol dissector crash in Wireshark 4.6.0 to 4.6.3 and 4.4.0 to 4.4.13 allows denial of service	5.5	More Details
CVE-2026-23999	Fleet is open source device management software. In versions prior to 4.80.1, Fleet generated device lock and wipe PINs using a predictable algorithm based solely on the current Unix timestamp. Because no secret key or additional entropy was used, the resulting PIN could potentially be derived if the approximate time the device was locked is known. Fleet’s device lock and wipe commands generate a 6-digit PIN that is displayed to administrators for unlocking a device. In affected versions, this PIN was deterministically derived from the current timestamp. An attacker with physical possession of a locked device and knowledge of the approximate time the lock command was issued could theoretically predict the correct PIN within a limited search window. However, successful exploitation is constrained by multiple factors: Physical access to the device is required, the approximate lock time must be known, the operating system enforces rate limiting on PIN entry attempts, attempts would need to be spread over, and device wipe operations would typically complete before sufficient attempts could be made. As a result, this issue does not allow remote exploitation, fleet-wide compromise, or bypass of Fleet authentication controls. Version 4.80.1 contains a patch. No known workarounds are available.	5.5	More Details
CVE-2026-20107	A vulnerability in the Object Model CLI component of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, local attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. To exploit this vulnerability, the attacker must have valid user credentials and any role that includes CLI access. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by issuing crafted commands at the CLI prompt. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	5.5	More Details
CVE-2025-48642	In jump_to_payload of payload.rs, there is a possible information disclosure due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
	wpForo Forum 2.4.14 contains a stored cross-site scripting vulnerability that allows script injection		

CVE-2026-28560	via forum URL data output into an inline script block using json_encode without the JSON_HEX_TAG flag. Attackers set a forum slug containing a closing script tag or unescaped single quote to break out of the JavaScript string context and execute arbitrary script in all visitors' browsers.	5.5	More Details
CVE-2026-28556	wpForo Forum 2.4.14 contains a missing authorization vulnerability that allows authenticated subscribers to move, merge, or split any forum topic via the topic_move, topic_merge, and topic_split form action handlers. Attackers with a valid form nonce can reorganize arbitrary forum content without moderator permissions, including relocating topics to private forums.	5.4	More Details
CVE-2026-24350	PluXml CMS is vulnerable to Stored XSS in file uploading functionality. An authenticated attacker can upload an SVG file containing a malicious payload, which will be executed when a victim clicks the link associated with the uploaded image. In version 5.9.0-rc7 clicking the link associated with the uploaded image doesn't execute malicious code but directly accessing the file will still execute the embedded payload. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 5.8.21 and 5.9.0-rc7 were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	5.4	More Details
CVE-2026-28357	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, a stored XSS vulnerability exists in the Formula virtual cell. Formula results containing URI::() patterns are rendered via v-html without sanitization, allowing injected HTML to execute. This issue has been patched in version 0.301.3.	5.4	More Details
CVE-2026-24351	PluXml CMS is vulnerable to Stored XSS in Static Pages editing functionality. Attacker with editing privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting edited page. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 5.8.21 and 5.9.0-rc7 were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	5.4	More Details
CVE-2026-28359	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, an authenticated user with Editor role can inject arbitrary HTML into Rich Text cells by bypassing the TipTap editor and sending raw HTML via the API. This issue has been patched in version 0.301.3.	5.4	More Details
CVE-2025-67491	OpenEMR is a free and open source electronic health records and medical practice management application. Versions 5.0.0.5 through 7.0.3.4 have a stored cross-site scripting vulnerability in the ub04 helper of the billing interface. The variable `$data` is passed in a click event handler enclosed in single quotes without proper sanitization. Thus, despite `json_encode` a malicious user can still inject a payload such as ` ac' ><img src=x onerror=alert(document.cookie)> ` to trigger the bug. This vulnerability allows low privileged users to embed malicious JS payloads on the server and perform stored XSS attack. This, in turn makes it possible for malicious users to steal the session cookies and perform unauthorized actions impersonating administrators. Version 7.0.4 patches the issue.	5.4	More Details
CVE-2026-28398	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, user-controlled content in comments and rich text cells was rendered via v-html without sanitization, enabling stored XSS. This issue has been patched in version 0.301.3.	5.4	More Details
CVE-2025-13734	IBM Engineering Requirements Management DOORS Next 7.1, and 7.2 could allow an authenticated user to view and edit data beyond their authorized access permissions.	5.4	More Details
CVE-2026-27948	Copyparty is a portable file server. In versions prior to 1.20.9, an XSS allows for reflected cross-site scripting via URL-parameter `?setck=...`. Version 1.20.9 fixes the issue.	5.4	More Details
CVE-2026-3268	A vulnerability was detected in psi-probe PSI Probe up to 5.3.0. The affected element is an unknown function of the file psi-probe-core/src/main/java/psiprobe/controllers/sessions/RemoveSessAttributeController.java of the component Session Attribute Handler. Performing a manipulation results in improper access controls. 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.	5.4	More Details
CVE-2026-	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 #59, a normal authenticated user can store the XSS payload. The payload is triggered by administrator. Version	5.4	More Details

26997	5.5.3 #59 fixes the issue.		
CVE-2026-27639	Mercator is an open source web application designed to enable mapping of information systems. A stored Cross-Site Scripting (XSS) vulnerability exists in Mercator prior to version 2026.02.22 due to the use of unescaped Blade directives (`{!! !!}`) in display templates. An authenticated user with the User role can inject arbitrary JavaScript payloads into fields such as "contact point" when creating or editing entities. The payload is then executed in the browser of any user who views the affected page, including administrators. Version 2026.02.22 fixes the vulnerability.	5.4	More Details
CVE-2026-20122	A vulnerability in the API of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to overwrite arbitrary files on the local file system. To exploit this vulnerability, the attacker must have valid read-only credentials with API access on the affected system. This vulnerability is due to improper file handling on the API interface of an affected system. An attacker could exploit this vulnerability by uploading a malicious file on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on the affected system and gain vmanage user privileges.	5.4	More Details
CVE-2026-26207	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, `discourse-policy` plugin allows any authenticated user to interact with policies on posts they do not have permission to view. The `PolicyController` loads posts by ID without verifying the current user's access, enabling policy group members to accept/unaccept policies on posts in private categories or PMs they cannot see and any authenticated user to enumerate which post IDs have policies attached via differentiated error responses (information disclosure). The issue is patched in versions 2025.12.2, 2026.1.1, and 2026.2.0 by adding a `guardian.can_see?(@post)` check in the `set_post` before_action, ensuring post visibility is verified before any policy action is processed. As a workaround, disabling the discourse-policy plugin (`policy_enabled = false`) eliminates the vulnerability. There is no other workaround without upgrading.	5.4	More Details
CVE-2025-64999	Improper neutralization of input in Checkmk versions 2.4.0 before 2.4.0p22, and 2.3.0 before 2.3.0p43 allows an attacker that can manipulate a host's check output to inject malicious JavaScript into the Synthetic Monitoring HTML logs, which can then be accessed via a crafted phishing link.	5.4	More Details
CVE-2026-27792	Seerr is an open-source media request and discovery manager for Jellyfin, Plex, and Emby. A missing authorization vulnerability has been identified in the application starting in version 2.7.0 and prior to version 3.1.0. It allows authenticated users to access and modify data belonging to other users. This issue is due to the absence of the `isOwnProfileOrAdmin()` middleware on several push subscription API routes. Version 3.1.0 fixes the issue.	5.4	More Details
CVE-2026-28397	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, comments rendered via v-html without sanitization enable stored XSS. This issue has been patched in version 0.301.3.	5.4	More Details
CVE-2025-56605	A reflected Cross-Site Scripting (XSS) vulnerability exists in the register.php backend script of PuneethReddyHC Event Management System 1.0. The mobile POST parameter is improperly validated and echoed back in the HTTP response without sanitization, allowing an attacker to inject and execute arbitrary JavaScript code in the victim's browser.	5.4	More Details
CVE-2026-28401	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, rich text cell content rendered via v-html without sanitization enables stored XSS. This issue has been patched in version 0.301.3.	5.4	More Details
CVE-2026-2694	The The Events Calendar plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to an improper capability check on the 'can_edit' and 'can_delete' function in all versions up to, and including, 6.15.16. This makes it possible for authenticated attackers, with Contributor-level access and above, to update or trash events, organizers and venues via REST API.	5.4	More Details
CVE-2026-27621	TypiCMS is a multilingual content management system based on the Laravel framework. A Stored Cross-Site Scripting (XSS) vulnerability exists in the file upload module of TypiCMS prior to version 16.1.7. The application allows users with file upload permissions to upload SVG files. While there is a MIME type validation, the content of the SVG file is not sanitized. An attacker can upload a specially crafted SVG file containing malicious JavaScript code. When another user (such as an administrator) views or accesses this file through the application, the script executes in their browser, leading to a compromise of that user's session. The issue is exacerbated by a bug in the	5.4	More Details

	SVG parsing logic, which can cause a 500 error if the uploaded SVG does not contain a `viewBox` attribute. However, this does not mitigate the XSS vulnerability, as an attacker can easily include a valid `viewBox` attribute in their malicious payload. Version 16.1.7 of TypiCMS Core fixes the issue.		
CVE-2026-28218	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, fail-open access control in Data Explorer plugin allows any authenticated user to execute SQL queries that have no explicit group assignments, including built-in system queries. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. As a workaround, either explicitly set group permissions on each Data Explorer query that doesn't have permissions, or disable discourse-data-explorer plugin.	5.4	More Details
CVE-2026-28358	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, the password forgot endpoint returned different responses for registered and unregistered emails, allowing user enumeration. This issue has been patched in version 0.301.3.	5.3	More Details
CVE-2026-2878	In Progress® Telerik® UI for AJAX, versions prior to 2026.1.225, an insufficient entropy vulnerability exists in RadAsyncUpload, where a predictable temporary identifier, based on timestamp and filename, can enable collisions and file content tampering.	5.3	More Details
CVE-2026-23865	An integer overflow in the tt_var_load_item_variation_store function of the Freetype library in versions 2.13.2 and 2.13.3 may allow for an out of bounds read operation when parsing HVAR/VVAR/MVAR tables in OpenType variable fonts. This issue is fixed in version 2.14.2.	5.3	More Details
CVE-2026-28360	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.3, shared view passwords were stored in plaintext in the database and compared using direct string equality. This issue has been patched in version 0.301.3.	5.3	More Details
CVE-2024-50337	Chamilo is a learning management system. Prior to version 1.11.28, the OpenId function allows anyone to send requests to any URL on server's behalf, which results in unauthenticated blind SSRF. This issue has been patched in version 1.11.28.	5.3	More Details
CVE-2026-3185	A vulnerability was found in feiyuchuixue sz-boot-parent up to 1.3.2-beta. Affected is an unknown function of the file /api/admin/sys-message/ of the component API Endpoint. The manipulation of the argument messageId results in authorization bypass. The attack can be launched remotely. The exploit has been made public and could be used. Upgrading to version 1.3.3-beta is able to address this issue. The patch is identified as aefaabfd7527188bfba3c8c9eee17c316d094802. The affected component should be upgraded. The project was informed beforehand and acted very professional: "We have implemented message ownership verification, so that users can only query messages related to themselves."	5.3	More Details
CVE-2026-28559	wpForo Forum 2.4.14 contains an information disclosure vulnerability that allows unauthenticated users to retrieve private and unapproved forum topics via the global RSS feed endpoint. Attackers request the RSS feed without a forum ID parameter, bypassing the privacy and status WHERE clauses that are only applied when a specific forum ID is present in the query.	5.3	More Details
CVE-2026-28407	malcontent is software for discovering supply-chain compromises through context, differential analysis, and YARA. Prior to version 1.21.0, malcontent would remove nested archives which failed to extract which could potentially leave malicious content. A better approach is to preserve these archives so that malcontent can attempt a best-effort scan of the archive bytes. Version 1.21.0 fixes the issue.	5.3	More Details
CVE-2026-25138	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. Prior to versions 35.8.3, 38.5.4, and 39.3.1, the WebUI login endpoint returns distinct error messages depending on whether a supplied username exists, allowing unauthenticated attackers to enumerate valid usernames. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	5.3	More Details
CVE-2026-27610	Parse Dashboard is a standalone dashboard for managing Parse Server apps. In versions 7.3.0-alpha.42 through 9.0.0-alpha.7, the `ConfigKeyCache` uses the same cache key for both master key and read-only master key when resolving function-typed keys. Under specific timing conditions, a read-only user can receive the cached full master key, or a regular user can receive the cached read-only master key. The fix in version 9.0.0-alpha.8 uses distinct cache keys for master key and read-only master key. As a workaround, avoid using function-typed master keys, or remove the `agent` configuration block from your dashboard configuration.	5.3	More Details
	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, a buffer		

CVE-2026-26271	overread in `freerdp_image_copy_from_icon_data()` (libfreerdp/codec/color.c) can be triggered by crafted RDP Window Icon (TS_ICON_INFO) data. The bug is reachable over the network when a client processes icon data from an RDP server (or from a man-in-the-middle). Version 3.23.0 fixes the issue.	5.3	More Details
CVE-2026-27951	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, the function `Stream_EnsureCapacity` can create an endless blocking loop. This may affect all client and server implementations using `FreeRDP`. For practical exploitation this will only work on 32bit systems where the available physical memory is `>= SIZE_MAX`. Version 3.23.0 contains a patch. No known workarounds are available.	5.3	More Details
CVE-2026-1305	The Japanized for WooCommerce plugin for WordPress is vulnerable to Improper Authentication in versions up to, and including, 2.8.4. This is due to a flawed permission check in the `paidy_webhook_permission_check` function that unconditionally returns `true` when the webhook signature header is omitted. This makes it possible for unauthenticated attackers to bypass payment verification and fraudulently mark orders as "Processing" or "Completed" without actual payment via a crafted POST request to the Paidy webhook endpoint.	5.3	More Details
CVE-2025-59060	Hostname verification bypass issue in Apache Ranger NiFiRegistryClient/NiFiClient is reported in Apache Ranger versions <= 2.7.0. Users are recommended to upgrade to version 2.8.0, which fixes this issue.	5.3	More Details
CVE-2026-1558	The WP Recipe Maker plugin for WordPress is vulnerable to an Insecure Direct Object Reference (IDOR) in versions up to, and including, 10.3.2. This is due to the /wp-json/wp-recipe-maker/v1/integrations/instacart REST API endpoint's permission_callback being set to __return_true and a lack of subsequent authorization or ownership checks on the user-supplied recipeId. This makes it possible for unauthenticated attackers to overwrite arbitrary post metadata (wprm_instacart_combinations) for any post ID on the site via the recipeId parameter.	5.3	More Details
CVE-2026-28421	Vim is an open source, command line text editor. Versions prior to 9.2.0077 have a heap-buffer-overflow and a segmentation fault (SEGV) exist in Vim's swap file recovery logic. Both are caused by unvalidated fields read from crafted pointer blocks within a swap file. Version 9.2.0077 fixes the issue.	5.3	More Details
CVE-2026-3281	A vulnerability was detected in libvips 8.19.0. This affects the function vips_bandrank_build of the file libvips/conversion/bandrank.c. Performing a manipulation of the argument index results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit is now public and may be used. The patch is named fd28c5463697712cb0ab116a2c55e4f4d92c4088. It is suggested to install a patch to address this issue.	5.3	More Details
CVE-2026-27884	NetExec is a network execution tool. Prior to version 1.5.1, the module spider_plus improperly creates the output file and folder path when saving files from SMB shares. It does not take into account that it is possible for Linux SMB shares to have path traversal characters such as `../` in them. An attacker can craft a filename in an SMB share that includes these characters, which when spider_plus crawls and downloads, can write or overwrite arbitrary files. The issue is patched in v1.5.1. As a workaround, do not run spider_plus with DOWNLOAD=true against targets.	5.3	More Details
CVE-2026-27824	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Prior to version 9.4.0, the calibre Content Server's brute-force protection mechanism uses a ban key derived from both `remote_addr` and the `X-Forwarded-For` header. Since the `X-Forwarded-For` header is read directly from the HTTP request without any validation or trusted-proxy configuration, an attacker can bypass IP-based bans by simply changing or adding this header, rendering the brute-force protection completely ineffective. This is particularly dangerous for calibre servers exposed to the internet, where brute-force protection is the primary defense against credential stuffing and password guessing attacks. Version 9.4.0 contains a fix for the issue.	5.3	More Details
CVE-2026-3137	A security vulnerability has been detected in CodeAstro Food Ordering System 1.0. This affects an unknown function of the file food_ordering.exe. Such manipulation leads to stack-based buffer overflow. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2026-	The AI ChatBot with ChatGPT and Content Generator by AYS plugin for WordPress is vulnerable to unauthorized access and modification of data due to missing capability checks on the store_data() and get_chatgpt_api_key() functions in all versions up to, and including, 2.7.5. This makes it	5.3	More Details

1336	possible for unauthenticated attackers to view, modify or delete the plugin's ChatGPT API key. The vulnerability was partially fixed in version 2.7.5 and fully fixed in version 2.7.6		
CVE-2026-24004	Fleet is open source device management software. In versions prior to 4.80.1, a vulnerability in Fleet’s Android MDM Pub/Sub handling could allow unauthenticated requests to trigger device unenrollment events. This may result in unauthorized removal of individual Android devices from Fleet management. If Android MDM is enabled, an attacker could send a crafted request to the Android Pub/Sub endpoint to unenroll a targeted Android device from Fleet without authentication. This issue does not grant access to Fleet, allow execution of commands, or provide visibility into device data. Impact is limited to disruption of Android device management for the affected device. Version 4.80.1 fixes the issue. If an immediate upgrade is not possible, affected Fleet users should temporarily disable Android MDM.	5.3	More Details
CVE-2026-28225	Manyfold is an open source, self-hosted web application for managing a collection of 3d models, particularly focused on 3d printing. Prior to version 0.133.1, the `get_model` method in `ModelFilesController` (line 158-160) loads models using `Model.find_param(params[:model_id])` without `policy_scope()`, bypassing Pundit authorization. All other controllers correctly use `policy_scope(Model).find_param()` (e.g., `ModelsController` line 263). Version 0.133.1 fixes the issue.	5.3	More Details
CVE-2026-2356	The User Registration & Membership – Custom Registration Form, Login Form, and User Profile plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.2 via the 'register_member' function, due to missing validation on the 'member_id' user controlled key. This makes it possible for unauthenticated attackers to delete arbitrary user accounts that newly registered on the site who has the 'urm_user_just_created' user meta set.	5.3	More Details
CVE-2026-27021	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, the voters endpoint in the poll plugin lacked post visibility checks which allowed unauthorized access to voters details of polls in any post. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	5.3	More Details
CVE-2026-28132	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in villatheme WooCommerce Photo Reviews woocommerce-photo-reviews allows Code Injection.This issue affects WooCommerce Photo Reviews: from n/a through <= 1.4.4.	5.3	More Details
CVE-2026-3145	A flaw has been found in libvips up to 8.18.0. The affected element is the function vips_foreign_load_matrix_file_is_a/vips_foreign_load_matrix_header of the file libvips/foreign/matrixload.c. Executing a manipulation can lead to memory corruption. The attack needs to be launched locally. This patch is called d4ce337c76bff1b278d7085c3c4f4725e3aa6ece. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2024-55023	Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 was discovered to contain a hardcoded encryption key which could allow attackers to access sensitive information.	5.3	More Details
CVE-2026-1725	GitLab has remediated an issue in GitLab CE/EE affecting versions from 18.9 before 18.9.1 that could have under certain conditions, allowed an unauthenticated user to cause denial of service by sending specially crafted requests to a CI jobs API endpoint.	5.3	More Details
CVE-2026-28351	pypdf is a free and open-source pure-python PDF library. Prior to version 6.7.4, an attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires parsing the content stream using the RunLengthDecode filter. This has been fixed in pypdf 6.7.4. As a workaround, consider applying the changes from PR #3664.	5.3	More Details
CVE-2026-28419	Vim is an open source, command line text editor. Prior to version 9.2.0075, a heap-based buffer underflow exists in Vim's Emacs-style tags file parsing logic. When processing a malformed tags file where a delimiter appears at the start of a line, Vim attempts to read memory immediately preceding the allocated buffer. Version 9.2.0075 fixes the issue.	5.3	More Details
CVE-2026-3147	A vulnerability was found in libvips up to 8.18.0. This affects the function vips_foreign_load_csv_build of the file libvips/foreign/csvload.c. The manipulation results in heap-based buffer overflow. The attack requires a local approach. The exploit has been made public and could be used. The patch is identified as b3ab458a25e0e261cbd1788474bbc763f7435780. It is advisable to implement a patch to correct this issue.	5.3	More Details
CVE-	Information Exposure Vulnerability in Hitachi Ops Center API Configuration Manager, Hitachi		

2025-5781	Configuration Manager, Hitachi Device Manager allows Session Hijacking.This issue affects Hitachi Ops Center API Configuration Manager: from 10.0.0-00 before 11.0.5-00; Hitachi Configuration Manager: from 8.5.1-00 before 11.0.5-00; Hitachi Device Manager: from 8.4.1-00 before 8.6.5-00.	5.2	More Details
CVE-2025-14480	IBM Aspera faspio Gateway 1.3.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information	5.1	More Details
CVE-2026-27900	The Terraform Provider for Linode versions prior to v3.9.0 logged sensitive information including some passwords, StackScript content, and object storage data in debug logs without redaction. Provider debug logging is not enabled by default. This issue is exposed when debug/provider logs are explicitly enabled (for example in local troubleshooting, CI/CD jobs, or centralized log collection). If enabled, sensitive values may be written to logs and then retained, shared, or exported beyond the original execution environment. An authenticated user with access to provider debug logs (through log aggregation systems, CI/CD pipelines, or debug output) would thus be able to extract these sensitive credentials. Versions 3.9.0 and later sanitize debug logs by logging only non-sensitive metadata such as labels, regions, and resource IDs while redacting credentials, tokens, keys, scripts, and other sensitive content. Some other mitigations and workarounds are available. Disable Terraform/provider debug logging or set it to `WARN` level or above, restrict access to existing and historical logs, purge/retention-trim logs that may contain sensitive values, and/or rotate potentially exposed secrets/credentials.	5.0	More Details
CVE-2026-22716	Out-of-bound write vulnerability in VMware Workstation 25H1 and below on any platform allows an actor with non-administrative privileges on a guest VM to terminate certain Workstation processes.	5.0	More Details
CVE-2025-9572	n authorization flaw in Foreman's GraphQL API allows low-privileged users to access metadata beyond their assigned permissions. Unlike the REST API, which correctly enforces access controls, the GraphQL endpoint does not apply proper filtering, leading to an authorization bypass.	5.0	More Details
CVE-2026-3404	A flaw has been found in thinkgem JeeSite up to 5.15.1. Impacted is an unknown function of the file /com/jeesite/common/shiro/cas/CasOutHandler.java of the component Endpoint. Executing a manipulation can lead to xml external entity reference. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is considered difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-27710	NanaZip is an open source file archive. Starting in version 5.0.1252.0 and prior to versions 6.0.1638.0 and 6.5.1638.0, a denial-of-service vulnerability exists in NanaZip's `.NET Single File Application` parser. A crafted bundle can force an integer underflow in header-size calculation and trigger an unbounded memory allocation attempt during archive open. Versions 6.0.1638.0 and 6.5.1638.0 fix the issue.	5.0	More Details
CVE-2025-68277	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 7.0.4, when a link is sent via Secure Messaging, clicking the link opens the website within the OpenEMR/Portal site. This behavior could be exploited for phishing. Version 7.0.4 patches the issue.	5.0	More Details
CVE-2026-2479	The Responsive Lightbox & Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.7.1. This is due to the use of `strpos()` for substring-based hostname validation instead of strict host comparison in the `ajax_upload_image()` function. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services.	5.0	More Details
CVE-2026-27600	HomeBox is a home inventory and organization system. Prior to 0.24.0-rc.1, the notifier functionality allows authenticated users to specify arbitrary URLs to which the application sends HTTP POST requests. No validation or restriction is applied to the supplied host, IP address, or port. Although the application does not return the response body from the target service, its UI behavior differs depending on the network state of the destination. This creates a behavioral side-channel that enables internal service enumeration. This vulnerability is fixed in 0.24.0-rc.1.	5.0	More Details
CVE-2026-27162	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, `posts_nearby` was checking topic access but then returning all posts regardless of type, including whispers that should only be visible to whisperers. Use `Post.secured(guardian)` to properly filter post types based on user permissions. Versions 2025.12.2, 2026.1.1, and	4.9	More Details

	2026.2.0 patch the issue. No known workarounds are available.		
CVE-2026-28270	Kiteworks is a private data network (PDN). Prior to version 9.2.0, a vulnerability in Kiteworks configuration allows uploading of arbitrary files without proper validation. Malicious administrators could exploit this to upload unauthorized file types to the system. Version 9.2.0 contains a patch for the issue.	4.9	More Details
CVE-2026-22728	Bitnami Sealed Secrets is vulnerable to a scope-widening attack during the secret rotation (/v1/rotate) flow. The rotation handler derives the sealing scope for the newly encrypted output from untrusted spec.template.metadata.annotations present in the input SealedSecret. By submitting a victim SealedSecret to the rotate endpoint with the annotation sealedsecrets.bitnami.com/cluster-wide=true injected into the template metadata, a remote attacker can obtain a rotated version of the secret that is cluster-wide. This bypasses original "strict" or "namespace-wide" constraints, allowing the attacker to retarget and unseal the secret in any namespace or under any name to recover the plaintext credentials.	4.9	More Details
CVE-2026-2831	The MailArchiver plugin for WordPress is vulnerable to SQL Injection via the ‘logid’ parameter in all versions up to, and including, 4.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-50198	Chamilo is a learning management system. Prior to version 1.11.30, Chamilo is vulnerable to deserialization of untrusted data in /plugin/vchamilo/views/import.php via POST configuration_file; POST course_path; POST home_path parameters. This issue has been patched in version 1.11.30.	4.9	More Details
CVE-2026-3221	Sensitive user account information is not encrypted in the database in Devolutions Server 2025.3.14 and earlier, which allows an attacker with access to the database to obtain sensitive user information via direct database access.	4.9	More Details
CVE-2026-0871	A flaw was found in Keycloak. An administrator with `manage-users` permission can bypass the "Only administrators can view" setting for unmanaged attributes, allowing them to modify these attributes. This improper access control can lead to unauthorized changes to user profiles, even when the system is configured to restrict such modifications.	4.9	More Details
CVE-2026-26228	VideoLAN VLC for Android prior to version 3.7.0 contains a path traversal vulnerability in the Remote Access Server routing for the authenticated endpoint GET /download. The file query parameter is concatenated into a filesystem path under the configured download directory without canonicalization or directory containment checks, allowing an authenticated attacker with network reachability to the Remote Access Server to request files outside the intended directory. The impact is bounded by the Android application sandbox and storage restrictions, typically limiting exposure to app-internal and app-specific external storage.	4.9	More Details
CVE-2026-26936	Inefficient Regular Expression Complexity (CWE-1333) in the AI Inference Anonymization Engine in Kibana can lead Denial of Service via Regular Expression Exponential Blowup (CAPEC-492).	4.9	More Details
CVE-2026-26698	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/modal_edit.php.	4.9	More Details
CVE-2026-26697	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_view.php?teacherID=.	4.9	More Details
CVE-2026-20091	A vulnerability in the web-based management interface of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious data into specific pages of the interface. 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. To exploit this vulnerability, the attacker must have valid credentials for a user account with the role of Administrator or AAA Administrator.	4.8	More Details
	Chamilo is a learning management system. Prior to version 1.11.30, a stored cross-site scripting		

CVE-2025-52470	(XSS) vulnerability exists in the session_category_add.php script. The vulnerability is caused by improper sanitization of the Category Name field, allowing privileged users to inject persistent JavaScript payloads. The injected script is later executed when accessing add_many_sessions_to_category.php, potentially compromising administrative sessions. This issue has been patched in version 1.11.30.	4.8	More Details
CVE-2025-50186	Chamilo is a learning management system. Prior to version 1.11.30, a stored cross-site scripting (XSS) vulnerability exists due to insufficient sanitization of CSV filenames. An attacker can upload a maliciously named CSV file (e.g., <img src=q onerror=prompt(8)>.csv) that leads to JavaScript execution when viewed by administrators or users with access to import logs or file views. This issue has been patched in version 1.11.30.	4.8	More Details
CVE-2026-27974	Audiobookshelf is a self-hosted audiobook and podcast server. A cross-site scripting (XSS) vulnerability exists in versions prior to 0.12.0-beta of the Audiobookshelf mobile application that allows arbitrary JavaScript execution through malicious library metadata. Attackers with library modification privileges (or control over a malicious podcast RSS feed) can execute code in victim users' WebViews, potentially leading to session hijacking, data exfiltration, and unauthorized access to native device APIs. audiobookshelf-app version 0.12.0-beta fixes the issue.	4.8	More Details
CVE-2026-27963	Audiobookshelf is a self-hosted audiobook and podcast server. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.32.0 of the Audiobookshelf web application that allows arbitrary JavaScript execution through malicious library metadata. Attackers with library modification privileges can execute code in victim users' browsers, potentially leading to session hijacking and data exfiltration. Version 2.32.0 contains a patch for the issue.	4.8	More Details
CVE-2026-25743	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, users with the "Forms administration" role can fill questionnaires ("forms") in patient encounters. The answers to the forms are displayed on the encounter page and in the visit history for the users with the same role. There exists a stored cross-site scripting (XSS) vulnerability in the function to display the form answers, allowing any authenticated attacker with the specific role to insert arbitrary JavaScript into the system by entering malicious payloads to the form answers. The JavaScript code is later executed by any user with the form role when viewing the form answers in the patient encounter pages or visit history. Version 8.0.0 fixes the issue.	4.8	More Details
CVE-2026-26717	An issue in OpenFUN Richie (LMS) in src/richie/apps/courses/api.py. The application used the non-constant time == operator for HMAC signature verification in the sync_course_run_from_request function. This allows remote attackers to forge valid signatures and bypass authentication by measuring response time discrepancies	4.8	More Details
CVE-2026-3486	A vulnerability has been found in itsourcecode College Management System 1.0. This vulnerability affects unknown code of the file /admin/student-fee.php. Such manipulation of the argument roll_no leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-0976	Information Exposure Vulnerability in Hitachi Ops Center API Configuration Manager, Hitachi Configuration Manager.This issue affects Hitachi Ops Center API Configuration Manager: from 10.0.0-00 before 11.0.4-00; Hitachi Configuration Manager: from 8.6.1-00 before 11.0.5-00.	4.7	More Details
CVE-2026-3202	NTS-KE protocol dissector crash in Wireshark 4.6.0 to 4.6.3 allows denial of service	4.7	More Details
CVE-2026-3201	USB HID protocol dissector memory exhaustion in Wireshark 4.6.0 to 4.6.3 and 4.4.0 to 4.4.13 allows denial of service	4.7	More Details
CVE-2025-14923	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.2 IBM WebSphere Application Server Liberty could provide weaker than expected security when using the Security Utility when administering security settings.	4.7	More Details
CVE-2026-3487	A vulnerability was found in itsourcecode College Management System 1.0. This issue affects some unknown processing of the file /admin/class-result.php. Performing a manipulation of the argument course_code results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-	Mattermost Desktop App versions <=5.13.3 fail to attach listeners restricting navigation to		

2026-1628	external sites within the Mattermost app which allows a malicious server to expose preload script functionality to untrusted servers via having a user open an external link in their Mattermost server. Mattermost Advisory ID: MMSA-2026-00596	4.6	More Details
CVE-2026-26272	HomeBox is a home inventory and organization system. Prior to 0.24.0-rc.1, a stored cross-site scripting (XSS) vulnerability exists in the item attachment upload functionality. The application does not properly validate or restrict uploaded file types, allowing an authenticated user to upload malicious HTML or SVG files containing executable JavaScript (also, potentially other formats that render scripts). Uploaded attachments are accessible via direct links. When a user accesses such a file in their browser, the embedded JavaScript executes in the context of the application's origin. This vulnerability is fixed in 0.24.0-rc.1.	4.6	More Details
CVE-2025-11563	URLs containing percent-encoded slashes (`/` or `\`) can trick wcurl into saving the output file outside of the current directory without the user explicitly asking for it. This flaw only affects the wcurl command line tool.	4.6	More Details
CVE-2026-20435	In preloader, there is a possible read of device unique identifiers due to a logic error. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10607099; Issue ID: MSV-6118.	4.6	More Details
CVE-2026-3194	A flaw has been found in Chia Blockchain 2.1.0. The affected element is the function send_transaction/get_private_key of the component RPC Server Master Passphrase Handler. This manipulation causes missing authentication. The attack can only be executed locally. The attack's complexity is rated as high. The exploitability is described as difficult. The exploit has been published and may be used. The vendor was informed early via email. A separate report via bugbounty was rejected with the reason "This is by design. The user is responsible for host security".	4.5	More Details
CVE-2026-25590	The GLPI Inventory Plugin handles network discovery, inventory, software deployment, and data collection for GLPI agents. Prior to 1.6.6, there is a reflected XSS vulnerability in task jobs. This vulnerability is fixed in 1.6.6.	4.5	More Details
CVE-2026-25135	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0 have an information disclosure vulnerability that leaks the entire contact information for all users, organizations, and patients in the system to anyone who has the system/(Group,Patient,*).$export operation and system/Location.read capabilities. This vulnerability will impact OpenEMR versions since 2023. This disclosure will only occur in extremely high trust environments as it requires using a confidential client with secure key exchange that requires an administrator to enable and grant permission before the app can even be used. This will typically only occur in server-server communication across trusted clients that already have established legal agreements. Version 8.0.0 contains a patch. As a workaround, disable clients that have the vulnerable scopes and only allow clients that do not have the system/Location.read scope until a fix has been deployed.	4.5	More Details
CVE-2026-20037	A vulnerability in the NX-OS CLI privilege levels of Cisco UCS Manager Software could allow an authenticated, local attacker with read-only privileges to modify files and perform unauthorized actions on an affected system. This vulnerability exists because unnecessary privileges are given to the user. An attacker could exploit this vulnerability by authenticating to a device as a read-only user and connecting to the NX-OS CLI. A successful exploit could allow the attacker to create or overwrite files in the file system or perform limited privileged actions on an affected device.	4.4	More Details
CVE-2026-2489	The TP2WP Importer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Watched domains' textarea on the attachment importer settings page in all versions up to, and including, 1.1. This is due to insufficient input sanitization and output escaping when domains are saved via AJAX and rendered with echo implode() without esc_textarea(). This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the attachment importer settings page.	4.4	More Details
CVE-2026-28417	Vim is an open source, command line text editor. Prior to version 9.2.0073, an OS command injection vulnerability exists in the `netrw` standard plugin bundled with Vim. By inducing a user to open a crafted URL (e.g., using the `scp://` protocol handler), an attacker can execute arbitrary shell commands with the privileges of the Vim process. Version 9.2.0073 fixes the issue.	4.4	More Details

CVE-2026-28418	Vim is an open source, command line text editor. Prior to version 9.2.0074, a heap-based buffer overflow out-of-bounds read exists in Vim's Emacs-style tags file parsing logic. When processing a malformed tags file, Vim can be tricked into reading up to 7 bytes beyond the allocated memory boundary. Version 9.2.0074 fixes the issue.	4.4	More Details
CVE-2026-20442	In display, there is a possible system crash due to use after free. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10436998; Issue ID: MSV-5723.	4.4	More Details
CVE-2026-20437	In MAE, there is a possible system crash due to use after free. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10431940; Issue ID: MSV-5843.	4.4	More Details
CVE-2026-20424	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5540.	4.4	More Details
CVE-2026-20445	In MDDP, there is a possible system crash due to a race condition. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10289875; Issue ID: MSV-5184.	4.4	More Details
CVE-2026-20439	In imgsys, there is a possible system crash due to use after free. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10431955; Issue ID: MSV-5826.	4.4	More Details
CVE-2026-2499	The Custom Logo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.2 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-2026-28420	Vim is an open source, command line text editor. Prior to version 9.2.0076, a heap-based buffer overflow WRITE and an out-of-bounds READ exist in Vim's terminal emulator when processing maximum combining characters from Unicode supplementary planes. Version 9.2.0076 fixes the issue.	4.4	More Details
CVE-2026-20429	In display, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10320471; Issue ID: MSV-5535.	4.4	More Details
CVE-2026-2498	The WP Social Meta plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-28195	In JetBrains TeamCity before 2025.11.3 missing authorization allowed project developers to add parameters to build configurations	4.3	More Details
CVE-2026-3269	A flaw has been found in psi-probe PSI Probe up to 5.3.0. The impacted element is the function handleRequestInternal of the file psi-probe-core/src/main/java/psiprobe/controllers/sessions/ExpireSessionsController.java of the component Session Handler. Executing a manipulation can lead to denial of service. 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.	4.3	More Details
CVE-2026-28554	wpForo Forum 2.4.14 contains a missing authorization vulnerability that allows authenticated subscribers to approve or unapprove any forum post via the wpforo_approve_ajax AJAX handler. Attackers exploit the nonce-only check by submitting a valid nonce with an arbitrary post ID to bypass moderation controls entirely.	4.3	More Details
	The Post Duplicator plugin for WordPress is vulnerable to unauthorized arbitrary protected post meta insertion in all versions up to, and including, 3.0.8. This is due to the `duplicate_post()` function in `includes/api.php` using `$wpdb->insert()` directly to the `wp_postmeta` table		

CVE-2026-2301	instead of WordPress's standard `add_post_meta()` function, which would call `is_protected_meta()` to prevent lower-privileged users from setting protected meta keys (those starting with `_`). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary protected post meta keys such as `_wp_page_template`, `_wp_attached_file`, and other sensitive meta keys on duplicated posts via the `customMetaData` JSON array parameter in the `/wp-json/post-duplicator/v1/duplicate-post` REST API endpoint.	4.3	More Details
CVE-2026-1747	GitLab has remediated an issue in GitLab EE affecting all versions from 17.11 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that, under certain conditions, could have allowed Developer-role users with insufficient privileges to make unauthorized modifications to protected Conan packages.	4.3	More Details
CVE-2026-28555	wpForo Forum 2.4.14 contains a missing authorization vulnerability that allows authenticated subscribers to close or reopen any forum topic via the wpforo_close_ajax handler. Attackers submit a valid nonce with an arbitrary topic ID to bypass the moderator permission requirement and disrupt forum discussions.	4.3	More Details
CVE-2026-2410	The Disable Admin Notices – Hide Dashboard Notifications plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.2. This is due to missing nonce validation in the `showPageContent()` function. This makes it possible for unauthenticated attackers to add arbitrary URLs to the blocked redirects list via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-3188	A security flaw has been discovered in feiyuchuixue sz-boot-parent up to 1.3.2-beta. This affects an unknown part of the file /api/admin/common/download/templates of the component API. Performing a manipulation of the argument templateName results in path traversal. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.3.3-beta is able to mitigate this issue. The patch is named aefaabfd7527188bfba3c8c9eee17c316d094802. It is recommended to upgrade the affected component. The project was informed beforehand and acted very professional: "We have implemented path validity checks on parameters for the template download interface (...)"	4.3	More Details
CVE-2026-27839	wger is a free, open-source workout and fitness manager. In versions up to and including 2.4, three `nutritional_values` action endpoints fetch objects via `Model.objects.get(pk=pk)` — a raw ORM call that bypasses the user-scoped queryset. Any authenticated user can read another user's private nutrition plan data, including caloric intake and full macro breakdown, by supplying an arbitrary PK. Commit 29876a1954fe959e4b58ef070170e81703dab60e contains a fix for the issue.	4.3	More Details
CVE-2025-14103	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.7 before 18.7.5, 18.8 before 18.8.5, and 18.9 before 18.9.1 that could have allowed an unauthorized user with Developer-role permissions to set pipeline variables for manually triggered jobs under certain conditions.	4.3	More Details
CVE-2026-28219	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, an improper authorization check in the topic management logic allows authenticated users to modify privileged attributes of their topics. By manipulating specific parameters in a PUT or POST request, a regular user can elevate a topic’s status to a site-wide notice or banner, bypassing intended administrative restrictions. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. There are no practical workarounds to prevent this behavior other than applying the security patch. Administrators concerned about unauthorized promotions should audit recent changes to site banners and global notices until the fix is deployed.	4.3	More Details
CVE-2026-27835	wger is a free, open-source workout and fitness manager. In versions up to and including 2.4, `RepetitionsConfigViewSet` and `MaxRepetitionsConfigViewSet` return all users' repetition config data because their `get_queryset()` calls `.all()` instead of filtering by the authenticated user. Any registered user can enumerate every other user's workout structure. Commit 1fda5690b35706bb137850c8a084ec6a13317b64 contains a fix for the issue.	4.3	More Details
CVE-2026-27457	Weblate is a web based localization tool. Prior to version 5.16.1, the REST API's `AddonViewSet` (`weblate/api/views.py`, line 2831) uses `queryset = Addon.objects.all()` without overriding `get_queryset()` to scope results by user permissions. This allows any authenticated user (or anonymous users if `REQUIRE_LOGIN` is not set) to list and retrieve ALL addons across all projects and components via `GET /api/addons/` and `GET /api/addons/{id}/`. Version 5.16.1 fixes the issue.	4.3	More Details
	A flaw was found in the FTP GVfs backend. A malicious FTP server can exploit this vulnerability by		

CVE-2026-28295	providing an arbitrary IP address and port in its passive mode (PASV) response. The client unconditionally trusts this information and attempts to connect to the specified endpoint, allowing the malicious server to probe for open ports accessible from the client's network.	4.3	More Details
CVE-2026-28415	Gradio is an open-source Python package designed for quick prototyping. Prior to version 6.6.0, the _redirect_to_target() function in Gradio's OAuth flow accepts an unvalidated _target_url query parameter, allowing redirection to arbitrary external URLs. This affects the /logout and /login/callback endpoints on Gradio apps with OAuth enabled (i.e. apps running on Hugging Face Spaces with gr.LoginButton). Starting in version 6.6.0, the _target_url parameter is sanitized to only use the path, query, and fragment, stripping any scheme or host.	4.3	More Details
CVE-2026-26973	Discourse is an open source discussion platform. Versions prior to 2025.12.2, 2026.1.1, and 2026.2.0 have an IDOR (Insecure Direct Object Reference) in `ReviewableNotesController`. When `enable_category_group_moderation` is enabled, a user belonging to a category moderation group can create or delete their own notes on **any** reviewable in the system, including reviewables in categories they do not moderate. The controller used an unscoped `Reviewable.find` and the `ensure_can_see` guard only checked whether the user could access the review queue in general, not whether they could access the specific reviewable. Only instances with `enable_category_group_moderation` enabled are affected. Staff users (admins/moderators) are not impacted as they already have access to all reviewables. The issue is patched in versions 2025.12.2, 2026.1.1, and 2026.2.0 by scoping the reviewable lookup through `Reviewable.viewable_by(current_user)`. As a workaround, disable the `enable_category_group_moderation` site setting. This removes the attack surface as only staff users will have access to the review queue.	4.3	More Details
CVE-2026-28296	A flaw was found in the FTP GVfs backend. A remote attacker could exploit this input validation vulnerability by supplying specially crafted file paths containing carriage return and line feed (CRLF) sequences. These unsanitized sequences allow the attacker to terminate intended FTP commands and inject arbitrary FTP commands, potentially leading to arbitrary code execution or other severe impacts.	4.3	More Details
CVE-2026-28194	In JetBrains TeamCity before 2025.11.3 open redirect was possible in the React project creation flow	4.3	More Details
CVE-2026-27695	zae-limiter is a rate limiting library using the token bucket algorithm. Prior to version 0.10.1, all rate limit buckets for a single entity share the same DynamoDB partition key (`namespace/ENTITY#{id}`). A high-traffic entity can exceed DynamoDB's per-partition throughput limits (~1,000 WCU/sec), causing throttling that degrades service for that entity — and potentially co-located entities in the same partition. Version 0.10.1 fixes the issue.	4.3	More Details
CVE-2025-14742	The WP Recipe Maker plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'ajax_search_recipes' and 'ajax_get_recipe' functions in all versions up to, and including, 10.2.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive recipe information including draft, pending, and private recipes that they shouldn't be able to access.	4.3	More Details
CVE-2026-27840	ZITADEL is an open source identity management platform. Starting in version 2.31.0 and prior to versions 3.4.7 and 4.11.0, opaque OIDC access tokens in the v2 format truncated to 80 characters are still considered valid. Zitadel uses a symmetric AES encryption for opaque tokens. The cleartext payload is a concatenation of a couple of identifiers, such as a token ID and user ID. Internally Zitadel has 2 different versions of token payloads. v1 tokens are no longer created, but are still verified as to not invalidate existing session after upgrade. The cleartext payload has a format of `<token_id>:<user_id>`. v2 tokens distinguished further where the `token_id` is of the format `v2_<oidc_session_id>-at_<access_token_id>`. V1 token authZ/N session data is retrieved from the database using the (simple) `token_id` value and `user_id` value. The `user_id` (called `subject` in some parts of our code) was used as being the trusted user ID. V2 token authZ/N session data is retrieved from the database using the `oidc_session_id` and `access_token_id` and in this case the `user_id` from the token is ignored and taken from the session data in the database. By truncating the token to 80 chars, the user_id is now missing from the cleartext of the v2 token. The back-end still accepts this for above reasons. This issue is not considered exploitable, but may look awkward when reproduced. The patch in versions 4.11.0 and 3.4.7 resolves the issue by verifying the `user_id` from the token against the session data from the database. No known workarounds are available.	4.3	More Details
	Packistry is a self-hosted Composer repository designed to handle PHP package distribution. Prior		

CVE-2026-27968	to version 0.13.0, RepositoryAwareController::authorize() verified token presence and ability, but did not enforce token expiration. As a result, an expired deploy token with the correct ability could still access repository endpoints (e.g., Composer metadata/download APIs). The fix in version 0.13.0 adds an explicit expiration check, and tests now test expired deploy tokens to ensure they are rejected.	4.3	More Details
CVE-2026-20797	A stack based buffer overflow exists in an API route of XWEB Pro version 1.12.1 and prior, enabling unauthenticated attackers to cause stack corruption and a termination of the program.	4.3	More Details
CVE-2026-27758	SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a cross-site request forgery vulnerability in its management interface that allows attackers to induce authenticated users into submitting forged requests. Attackers can craft malicious requests that execute unauthorized configuration or administrative actions with the victim's privileges when the authenticated user visits a malicious webpage.	4.3	More Details
CVE-2026-3302	A weakness has been identified in SourceCodester Doctor Appointment System 1.0. Affected by this issue is some unknown functionality of the file /register.php of the component Sign Up Page. Executing a manipulation of the argument Email can lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-3408	A vulnerability was identified in Open Babel up to 3.1.1. This impacts the function OBAtom::GetExplicitValence of the file isrc/atom.cpp of the component CDXML File Handler. Such manipulation leads to null pointer dereference. The attack can be launched remotely. The exploit is publicly available and might be used. The name of the patch is e23a224b8fd9d7c2a7cde9ef4ec6afb4c05aa08a. It is best practice to apply a patch to resolve this issue.	4.3	More Details
CVE-2026-3412	A vulnerability was detected in itsourcecode University Management System 1.0. This affects an unknown part of the file /att_single_view.php. The manipulation of the argument dt results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-1265	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to writing of sensitive Information in a log file.	4.3	More Details
CVE-2026-3494	In MariaDB server version through 11.8.5, when server audit plugin is enabled with server_audit_events variable configured with QUERY_DCL, QUERY_DDL, or QUERY_DML filtering, if an authenticated database user invokes a SQL statement prefixed with double-hyphen (—) or hash (#) style comments, the statement is not logged.	4.3	More Details
CVE-2026-25941	FreeRDP is a free implementation of the Remote Desktop Protocol. Versions on the 2.x branch prior to to 2.11.8 and on the 3.x branch prior to 3.23.0 have an out-of-bounds read vulnerability in the FreeRDP client's RDPGFX channel that allows a malicious RDP server to read uninitialized heap memory by sending a crafted WIRE_TO_SURFACE_2 PDU with a `bitmapDataLength` value larger than the actual data in the packet. This can lead to information disclosure or client crashes when a user connects to a malicious server. Versions 2.11.8 and 3.23.0 fix the issue.	4.3	More Details
CVE-2026-27795	LangChain is a framework for building LLM-powered applications. Prior to version 1.1.8, a redirect-based Server-Side Request Forgery (SSRF) bypass exists in `RecursiveUrlLoader` in `@langchain/community`. The loader validates the initial URL but allows the underlying fetch to follow redirects automatically, which permits a transition from a safe public URL to an internal or metadata endpoint without revalidation. This is a bypass of the SSRF protections introduced in 1.1.14 (CVE-2026-26019). Users should upgrade to `@langchain/community` 1.1.18, which validates every redirect hop by disabling automatic redirects and re-validating `Location` targets before following them. In this version, automatic redirects are disabled (`redirect: "manual"`), each 3xx `Location` is resolved and validated with `validateSafeUrl()` before the next request, and a maximum redirect limit prevents infinite loops.	4.1	More Details
CVE-2026-0024	In isRedactionNeededForOpenViaContentResolver of MediaProvider.java, there is a possible way to reveal the location of media due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
	ImageMagick is free and open-source software used for editing and manipulating digital images.		

CVE-2026-27799	Prior to versions 7.1.2-15 and 6.9.13-40, a heap buffer over-read vulnerability exists in the DJVU image format handler. The vulnerability occurs due to integer truncation when calculating the stride (row size) for pixel buffer allocation. The stride calculation overflows a 32-bit signed integer, resulting in an out-of-bounds memory reads. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	4.0	More Details
CVE-2026-27798	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap buffer over-read vulnerability occurs when processing an image with small dimension using the `-wavelet-denoise` operator. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	4.0	More Details
CVE-2026-27973	Audiobookshelf is a self-hosted audiobook and podcast server. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 0.12.0-beta of the Audiobookshelf mobile application that allows arbitrary JavaScript execution through malicious library metadata. Attackers with library modification privileges can execute code in victim users' browsers/WebViews, potentially leading to session hijacking, data exfiltration, and unauthorized access to native device APIs. The issue is fixed in audiobookshelf-app version 0.12.0-beta, corresponding to audiobookshelf version 2.12.0.	4.0	More Details
CVE-2026-27150	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, missing `validate_before_create` authorization in Data Explorer's `QueryGroupBookmarkable` allows any logged-in user to create bookmarks for query groups they don't have access to, enabling metadata disclosure via bookmark reminder notifications. Versions 2025.12.2, 2026.1.1, and 2026.2.0 fix this issue and also make sure `validate_before_create` throws NotImplementedError in BaseBookmarkable if not implemented, to prevent similar issues in the future. No known workarounds are available.	3.8	More Details
CVE-2026-27152	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, DM communication-preference bypass when adding members via `Chat::AddUsersToChannel` — a user could add targets who have blocked/ignored/muted them to an existing DM channel, bypassing per-recipient PM restrictions that are enforced during DM channel creation. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	3.8	More Details
CVE-2025-67860	A vulnerability has been identified in the NeuVector scanner where the scanner process accepts registry and controller credentials as command-line arguments, potentially exposing sensitive credentials to local users.	3.8	More Details
CVE-2026-23748	Golioth Firmware SDK version 0.10.0 prior to 0.22.0, fixed in commit d7f55b38, contain an out-of-bounds read in LightDB State string parsing. When processing a string payload, a payload_size value less than 2 can cause a size_t underflow when computing the number of bytes to copy (nbytes). The subsequent memcpy() reads past the end of the network buffer, which can crash the device. The condition is reachable from on_payload, and golioth_payload_is_null() does not block payload_size==1. A malicious server or MITM can trigger a denial of service.	3.7	More Details
CVE-2026-26227	VideoLAN VLC for Android prior to version 3.7.0 contains an authentication bypass in the Remote Access Server feature due to missing or insufficient rate limiting on one-time password (OTP) verification. The Remote Access Server uses a 4-digit OTP and does not enforce effective throttling or lockout within the OTP validity window, allowing an attacker with network reachability to the server to repeatedly attempt OTP verification until a valid user_session cookie is issued. Successful exploitation results in unauthorized access to the Remote Access interface, limited to media files explicitly shared by the VLC for Android user.	3.7	More Details
CVE-2026-23747	Golioth Firmware SDK version 0.10.0 prior to 0.22.0, fixed in commit 48f521b, contain a stack-based buffer overflow in Payload Utils. The golioth_payload_as_int() and golioth_payload_as_float() helpers copy network-supplied payload data into fixed-size stack buffers using memcpy() with a length derived from payload_size. The only length checks are guarded by assert(); in release builds, the asserts are compiled out and memcpy() may copy an unbounded payload_size. Payloads larger than 12 bytes (int) or 32 bytes (float) can overflow the stack, resulting in a crash/denial of service. This is reachable via LightDB State on_payload with a malicious server or MITM.	3.7	More Details
CVE-2025-15598	A vulnerability was found in Dataease SQLBot up to 1.5.1. This impacts the function validateEmbedded of the file backend/apps/system/middleware/auth.py of the component JWT Token Handler. Performing a manipulation results in improper verification of cryptographic signature. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is said to be difficult. The exploit has been made public and could be used. A comment in the source code warns users about using this feature. The vendor was contacted	3.7	More Details

	early about this disclosure.		
CVE-2026-22877	An arbitrary file-read vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling unauthenticated attackers to read arbitrary files on the system, and potentially causing a denial-of-service attack.	3.7	More Details
CVE-2026-25674	An issue was discovered in 6.0 before 6.0.3, 5.2 before 5.2.12, and 4.2 before 4.2.29. Race condition in file-system storage and file-based cache backends in Django allows an attacker to cause file system objects to be created with incorrect permissions via concurrent requests, where one thread's temporary `umask` change affects other threads in multi-threaded environments. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Tarek Nakkouch for reporting this issue.	3.7	More Details
CVE-2026-0995	An issue has been identified in Arm C1-Pro before r1p2-50eac0, where, under certain conditions, a TLBI+DSB might fail to ensure the completion of memory accesses related to SME.	3.6	More Details
CVE-2026-3171	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /queue.php. This manipulation of the argument firstname/lastname causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2026-3382	A security flaw has been discovered in ChaiScript up to 6.1.0. The impacted element is the function chaiscript::Boxed_Number::get_as of the file include/chaiscript/dispatchkit/boxed_number.hpp. Performing a manipulation results in memory corruption. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3394	A vulnerability was detected in jarikomppa soloud up to 20200207. This affects the function SoLoud::Wav::loadwav of the file src/audiosource/wav/soloud_wav.cpp of the component WAV File Parser. Performing a manipulation results in memory corruption. The attack must be initiated from a local position. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3393	A security vulnerability has been detected in jarikomppa soloud up to 20200207. The impacted element is the function SoLoud::Wav::loadflac of the file src/audiosource/wav/soloud_wav.cpp of the component Audio File Handler. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3387	A vulnerability has been found in wren-lang wren up to 0.4.0. Affected by this issue is the function getByteCountForArguments of the file src/vm/wren_compiler.c. Such manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3386	A flaw has been found in wren-lang wren up to 0.4.0. Affected by this vulnerability is the function emitOp of the file src/vm/wren_compiler.c. This manipulation causes out-of-bounds read. It is possible to launch the attack on the local host. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3146	A vulnerability has been found in libvips up to 8.18.0. The impacted element is the function vips_foreign_load_matrix_header of the file libvips/foreign/matrixload.c. The manipulation leads to null pointer dereference. The attack needs to be performed locally. The identifier of the patch is d4ce337c76bff1b278d7085c3c4f4725e3aa6ece. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-3282	A flaw has been found in libvips 8.19.0. This vulnerability affects the function vips_unpremultiply_build of the file libvips/conversion/unpremultiply.c. Executing a manipulation of the argument alpha_band can lead to out-of-bounds read. The attack needs to be launched locally. The exploit has been published and may be used. This patch is called 7215ead1e0cd7d3703cc4f5fca06d7d0f4c22b91. A patch should be applied to remediate this issue.	3.3	More Details
	A security vulnerability has been detected in ChaiScript up to 6.1.0. This impacts the function		

CVE-2026-3384	chaiscript::eval::AST_Node_Impl::eval/chaiscript::eval::Function_Push_Pop of the file include/chaiscript/language/chaiscript_eval.hpp. The manipulation leads to uncontrolled recursion. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3388	A vulnerability was found in Squirrel up to 3.2. This affects the function SQCompiler::Factor/SQCompiler::UnaryOP of the file squirrel/sqcompiler.cpp. Performing a manipulation results in uncontrolled recursion. The attack needs to be approached locally. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3293	A weakness has been identified in snowflakedb snowflake-jdbc up to 4.0.1. Impacted is the function SdkProxyRoutePlanner of the file src/main/java/net/snowflake/client/internal/core/SdkProxyRoutePlanner.java of the component JDBC URL Handler. Executing a manipulation of the argument nonProxyHosts can lead to inefficient regular expression complexity. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. This patch is called 5fb0a8a318a2ed87f4022a1f56e742424ba94052. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-3389	A vulnerability was determined in Squirrel up to 3.2. This vulnerability affects the function sqstd_rex_newnode in the library sqstdlib/sqstdrex.cpp. Executing a manipulation can lead to null pointer dereference. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3449	Versions of the package @tootallnate/once before 3.0.1 are vulnerable to Incorrect Control Flow Scoping in promise resolving when AbortSignal option is used. The Promise remains in a permanently pending state after the signal is aborted, causing any await or .then() usage to hang indefinitely. This can cause a control-flow leak that can lead to stalled requests, blocked workers, or degraded application availability.	3.3	More Details
CVE-2026-3463	A weakness has been identified in xlnt-community xlnt up to 1.6.1. Impacted is the function xlnt::detail::binary_writer::append of the file source/detail/binary.hpp of the component Compound Document Parser. This manipulation causes heap-based buffer overflow. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. Patch name: 147. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2026-3285	A vulnerability was determined in berry-lang berry up to 1.1.0. The affected element is the function scan_string of the file src/be_lexer.c. This manipulation causes out-of-bounds read. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Patch name: 7149c59a39ba44feca261b12f06089f265fec176. Applying a patch is the recommended action to fix this issue.	3.3	More Details
CVE-2026-3385	A vulnerability was detected in wren-lang wren up to 0.4.0. Affected is the function resolveLocal of the file src/vm/wren_compiler.c. The manipulation results in uncontrolled recursion. Attacking locally is a requirement. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3284	A vulnerability was found in libvips 8.19.0. Impacted is the function vips_extract_area_build of the file libvips/conversion/extract.c. The manipulation of the argument extract_area results in integer overflow. The attack requires a local approach. The exploit has been made public and could be used. The patch is identified as 24795bb3d19d84f7b6f5ed86451ad556c8f2fe70. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-3283	A vulnerability has been found in libvips 8.19.0. This issue affects the function vips_extract_band_build of the file libvips/conversion/extract.c. The manipulation of the argument extract_band leads to out-of-bounds read. The attack needs to be performed locally. The exploit has been disclosed to the public and may be used. The identifier of the patch is 24795bb3d19d84f7b6f5ed86451ad556c8f2fe70. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-3390	A vulnerability was identified in FascinatedBox lily up to 2.3. This issue affects the function patch_line_end of the file src/lily_build_error.c of the component Error Reporting. The manipulation leads to out-of-bounds read. The attack can only be performed from a local environment. The exploit is publicly available and might be used. The project was informed of the problem early	3.3	More Details

	through an issue report but has not responded yet.		
CVE-2026-3391	A security flaw has been discovered in FascinatedBox lily up to 2.3. Impacted is the function clear_storages of the file src/lily_emitter.c. The manipulation results in out-of-bounds read. The attack is only possible with local access. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3392	A weakness has been identified in FascinatedBox lily up to 2.3. The affected element is the function eval_tree of the file src/lily_emitter.c. This manipulation causes null pointer dereference. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3383	A weakness has been identified in ChaiScript up to 6.1.0. This affects the function chaiscript::Boxed_Number::go of the file include/chaiscript/dispatchkit/boxed_number.hpp. Executing a manipulation can lead to divide by zero. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-3407	A vulnerability was determined in YosysHQ yosys up to 0.62. This affects the function Yosys::RTLIL::Const::set of the file kernel/rtlil.h of the component BLIF File Parser. This manipulation causes heap-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. Applying a patch is the recommended action to fix this issue. It appears that the issue is not reproducible all the time.	3.3	More Details
CVE-2026-3193	A vulnerability was detected in Chia Blockchain 2.1.0. Impacted is an unknown function of the file /send_transaction. The manipulation results in cross-site request forgery. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is considered difficult. The exploit is now public and may be used. The vendor was informed early via email. A separate report via bugbounty was rejected with the reason "This is by design. The user is responsible for host security".	3.1	More Details
CVE-2026-3405	A vulnerability has been found in thinkgem JeeSite up to 5.15.1. The affected element is an unknown function of the component Connection Handler. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is described 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.	3.1	More Details
CVE-2026-3401	A weakness has been identified in SourceCodester Web-based Pharmacy Product Management System 1.0. This affects an unknown part. This manipulation causes session expiration. Remote exploitation of the attack is possible. The complexity of an attack is rather high. It is indicated that the exploitability is difficult. The exploit has been made available to the public and could be used for attacks.	3.1	More Details
CVE-2026-3189	A weakness has been identified in feiyuchuixue sz-boot-parent up to 1.3.2-beta. This vulnerability affects unknown code of the file /api/admin/common/files/download. Executing a manipulation of the argument url can lead to server-side request forgery. The attack can be executed remotely. Attacks of this nature are highly complex. It is stated that the exploitability is difficult. Upgrading to version 1.3.3-beta is able to resolve this issue. This patch is called aefaabfd7527188bfba3c8c9eee17c316d094802. Upgrading the affected component is advised. The project was informed beforehand and acted very professional: "We have added a URL protocol whitelist validation to the file download interface, allowing only http and https protocols."	3.1	More Details
CVE-2025-12150	A flaw was found in Keycloak’s WebAuthn registration component. This vulnerability allows an attacker to bypass the configured attestation policy and register untrusted or forged authenticators via submission of an attestation object with fmt: "none", even when the realm is configured to require direct attestation. This can lead to weakened authentication integrity and unauthorized authenticator registration.	3.1	More Details
CVE-2026-27838	wger is a free, open-source workout and fitness manager. Five routine detail action endpoints check a cache before calling `self.get_object()`. In versions up to and including 2.4, ache keys are scoped only by `pk` — no user ID is included. When a victim has previously accessed their routine via the API, an attacker can retrieve the cached response for the same PK without any ownership check. Commit e964328784e2ee2830a1991d69fadbce86ac9fbf contains a patch for the issue.	3.1	More Details

CVE-2026-3465	A vulnerability was determined in Tuya App and SDK 24.07.11 on Android. Affected by this vulnerability is an unknown functionality of the component JSON Data Point Handler. This manipulation of the argument cruise_time causes denial of service. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been publicly disclosed and may be utilized. There is ongoing doubt regarding the real existence of this vulnerability. The vendor disagrees with the conclusion of the finding: "The described vulnerability fails to prove its feasibility or exploitability by attackers. The issue essentially does not constitute a security vulnerability, aligning more closely with abnormal product functionality." These considerations are properly reflected within the CVSS vector.	3.1	More Details
CVE-2026-23749	Golioth Firmware SDK version 0.19.1 prior to 0.22.0, fixed in commit 0e788217, contain an out-of-bounds read due to improper null termination of a blockwise transfer path. blockwise_transfer_init() accepts a path whose length equals CONFIG_GOLIOTH_COAP_MAX_PATH_LEN and copies it using strncpy() without guaranteeing a trailing NUL byte, leaving ctx->path unterminated. A later strlen() on this buffer (in golioth_coap_client_get_internal()) can read past the end of the allocation, resulting in a crash/denial of service. The input is application-controlled (not network by default).	2.9	More Details
CVE-2026-26887	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_supplier.php.	2.7	More Details
CVE-2026-26888	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_stock.php.	2.7	More Details
CVE-2026-26884	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/admin/appointments/view_appointment.php.	2.7	More Details
CVE-2026-26889	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_category.php.	2.7	More Details
CVE-2026-26891	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_parcel_type.php.	2.7	More Details
CVE-2026-26979	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, TL4 users are able to close, archive and pin topics in private categories they don't have access to. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	2.7	More Details
CVE-2026-26885	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /classes/Master.php?f=delete_service.	2.7	More Details
CVE-2026-27151	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, the `move_posts` action only checked `can_move_posts?` on the source topic but never validated write permissions on the destination topic. This allowed TL4 users and category group moderators to move posts into topics in categories where they lack posting privileges (e.g., read-only categories or categories with group-restricted write access). Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	2.7	More Details
CVE-2026-27153	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, moderators could export user Chat DMs via the CSV export endpoint by exploiting an overly permissive allowlist in `can_export_entity?`. The method allowed moderators to export any entity not explicitly blocked instead of restricting to an explicit allowlist. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.	2.7	More Details
CVE-2026-26883	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/classes/Master.php?f=delete_appointment.	2.7	More Details
CVE-2026-	Discourse is an open source discussion platform. Prior to versions 2025.12.2, 2026.1.1, and 2026.2.0, TL4 users can publish topics into staff-only categories via the `publish_to_category`	2.7	More

28227	topic timer, bypassing authorization checks. Versions 2025.12.2, 2026.1.1, and 2026.2.0 patch the issue. No known workarounds are available.		Details
CVE-2026-22717	Out-of-bound read vulnerability in VMware Workstation 25H1 and below on any platform allows an actor with non-administrative privileges on a guest VM to obtain limited information disclosure from the machine where VMware Workstation is installed.	2.7	More Details
CVE-2026-26890	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_product.php.	2.7	More Details
CVE-2026-21725	A time-of-create-to-time-of-use (TOCTOU) vulnerability lets recently deleted-then-recreated data sources be re-deleted without permission to do so. This requires several very stringent conditions to be met: - The attacker must have admin access to the specific datasource prior to its first deletion. - Upon deletion, all steps within the attack must happen within the next 30 seconds and on the same pod of Grafana. - The attacker must delete the datasource, then someone must recreate it. - The new datasource must not have the attacker as an admin. - The new datasource must have the same UID as the prior datasource. These are randomised by default. - The datasource can now be re-deleted by the attacker. - Once 30 seconds are up, the attack is spent and cannot be repeated. - No datasource with any other UID can be attacked.	2.6	More Details
CVE-2026-27632	Talishar is a fan-made Flesh and Blood project. Prior to commit 6be3871a14c192d1fb8146cdbc76f29f27c1cf48, the Talishar application lacks Cross-Site Request Forgery (CSRF) protections on critical state-changing endpoints, specifically within `SubmitChat.php` and other game interaction handlers. By failing to require unique, unpredictable session tokens, the application allows third-party malicious websites to forge requests on behalf of authenticated users, leading to unauthorized actions within active game sessions. The attacker would need to know both the proper gameName and playerID for the player. The player would also need to be browsing and interact with the infected website while playing a game. The vulnerability is fixed in commit 6be3871a14c192d1fb8146cdbc76f29f27c1cf48.	2.6	More Details
CVE-2026-20757	Improper Locking vulnerability (CWE-667) in Gallagher Morpho integration allows a privileged operator to cause a limited denial-of-service in the Command Centre Server. This issue affects Command Centre Server: 9.40 prior to vEL9.40.1976(MR1), 9.30 prior to vEL9.30.3382 (MR4), 9.20 prior to vEL9.20.3783 (MR6), 9.10 prior to vEL9.10.4647 (MR9), all versions of 9.00 and prior.	2.5	More Details
CVE-2026-3170	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected is an unknown function of the file /patient-search.php. The manipulation of the argument First Name/Last Name results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-3402	A security vulnerability has been detected in PHPGurukul Student Record Management System up to 1.0. This vulnerability affects unknown code of the file /edit-course.php. Such manipulation of the argument Course Short Name leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2026-3403	A vulnerability was detected in PHPGurukul Student Record Management System 1.0. This issue affects some unknown processing of the file /edit-subject.php. Performing a manipulation of the argument Subject 1 results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-28196	In JetBrains TeamCity before 2025.11.3 disabling versioned settings left a credentials config on disk	2.3	More Details
CVE-2026-28422	Vim is an open source, command line text editor. Prior to version 9.2.0078, a stack-buffer-overflow occurs in `build_stl_str_hl()` when rendering a statusline with a multi-byte fill character on a very wide terminal. Version 9.2.0078 patches the issue.	2.2	More Details
CVE-2023-31044	An issue was discovered in Nokia Impact before Mobile 23_FP1. In Impact DM 19.11 onwards, a remote authenticated user, using the Add Campaign functionality, can inject a malicious payload within the Campaign Name. This data can be exported to a CSV file. Attackers can populate data fields that may attempt data exfiltration or other malicious activity when automatically executed by the spreadsheet software.	2.0	More Details
	Gradio is an open-source Python package designed for quick prototyping. Starting in version		

CVE-2026-27167	4.16.0 and prior to version 6.6.0, Gradio applications running outside of Hugging Face Spaces automatically enable "mocked" OAuth routes when OAuth components (e.g. `gr.LoginButton`) are used. When a user visits `/login/huggingface`, the server retrieves its own Hugging Face access token via `huggingface_hub.get_token()` and stores it in the visitor's session cookie. If the application is network-accessible, any remote attacker can trigger this flow to steal the server owner's HF token. The session cookie is signed with a hardcoded secret derived from the string `"-v4"`, making the payload trivially decodable. Version 6.6.0 fixes the issue.	0.0	More Details
CVE-2026-24005	Kruise provides automated management of large-scale applications on Kubernetes. Prior to versions 1.8.3 and 1.7.5, PodProbeMarker allows defining custom probes with TCPSocket or HTTPGet handlers. The webhook validation does not restrict the Host field in these probe configurations. Since kruise-daemon runs with hostNetwork=true, it executes probes from the node network namespace. An attacker with PodProbeMarker creation permission can specify arbitrary Host values to trigger SSRF from the node, perform port scanning, and receive response feedback through NodePodProbe status messages. Versions 1.8.3 and 1.7.5 patch the issue.	0.0	More Details
CVE-2025-70236	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetDomainFilter.	N/A	More Details
CVE-2026-3342	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow an authenticated privileged administrator to execute arbitrary code with root permissions via an exposed management interface. This vulnerability affects Fireware OS 11.9 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.7 and 2025.1 up to and including 2026.1.1.	N/A	More Details
CVE-2025-70241	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWANType_Wizard5.	N/A	More Details
CVE-2026-3351	Improper authorization in the API endpoint GET /1.0/certificates in Canonical LXD 6.6 on Linux allows an authenticated, restricted user to enumerate all certificate fingerprints trusted by the lxd server.	N/A	More Details
CVE-2026-0869	Authentication bypass in Brocade ASCG 3.4.0 Could allow an unauthorized user to perform ASCG operations related to Brocade Support Link(BSL) and streaming configuration. and could even disable the ASCG application or disable use of BSL data collection on Brocade switches within the fabric.	N/A	More Details
CVE-2026-26892	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_carrier.php.	N/A	More Details
CVE-2026-29022	dr_libs version 0.14.4 and earlier (fixed in commit 8a7258c) contain a heap buffer overflow vulnerability in the drwav__read_smpl_to_metadata_obj() function of dr_wav.h that allows memory corruption via crafted WAV files. Attackers can exploit a mismatch between sampleLoopCount validation in pass 1 and unconditional processing in pass 2 to overflow heap allocations with 36 bytes of attacker-controlled data through any drwav_init_*_with_metadata() call on untrusted input.	N/A	More Details
CVE-2026-2915	HP System Event Utility might allow denial of service with elevated arbitrary file writes. This potential vulnerability was remediated with HP System Event Utility version 3.2.16.	N/A	More Details
CVE-2025-70234	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetQoS.	N/A	More Details
CVE-2025-70239	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard55.	N/A	More Details
CVE-2026-3344	A vulnerability in WatchGuard Fireware OS may allow an attacker to bypass the Fireware OS filesystem integrity check and maintain limited persistence via a maliciously-crafted firmware update package.This issue affects Fireware OS 12.0 up to and including 12.11.7, 12.5.9 up to and including 12.5.16, and 2025.1 up to and including 2026.1.1.	N/A	More Details

CVE-2025-70240	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard51.	N/A	More Details
CVE-2026-1775	The Labkotec LID-3300IP has an existing vulnerability in the ice detector software that enables an unauthenticated attacker to alter device parameters and run operational commands when specially crafted packets are sent to the device.	N/A	More Details
CVE-2026-21866	Dify is an open-source LLM app development platform. Prior to 1.11.2, Dify is vulnerable to a stored XSS issue when rendering Mermaid diagrams within chats. This occurs because Dify's default Mermaid configuration uses securityLevel: loose, which allows potentially unsafe content to execute. This vulnerability is fixed in 1.11.2.	N/A	More Details
CVE-2026-24415	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contains Reflected XSS vulnerabilities in invoice/order/contract modification modals. The application fails to properly sanitize user-supplied input from the righe GET parameter before reflecting it in HTML output.The $_GET['righe'] parameter is directly echoed into the HTML value attribute without any sanitization using htmlspecialchars() or equivalent functions. This allows an attacker to break out of the attribute context and inject arbitrary HTML/JavaScript.	N/A	More Details
CVE-2026-24848	OpenEMR is a free and open source electronic health records and medical practice management application. In 7.0.4 and earlier, the disposeDocument() method in EtherFaxActions.php allows authenticated users to write arbitrary content to arbitrary locations on the server filesystem. This vulnerability can be exploited to achieve Remote Code Execution (RCE) by uploading malicious PHP web shells.	N/A	More Details
CVE-2026-2590	Improper enforcement of the Disable password saving in vaults setting in the connection entry component in Devolutions Remote Desktop Manager 2025.3.30 and earlier allows an authenticated user to persist credentials in vault entries, potentially exposing sensitive information to other users, by creating or editing certain connection types while password saving is disabled.	N/A	More Details
CVE-2026-3130	Improper Enforcement of Behavioral Controls in Devolutions Server 2025.3.15 and earlier allows an authenticated attacker with the delete permission to delete a PAM account that is currently checked out by selecting it alongside at least one non-checked-out account and performing a bulk deletion.	N/A	More Details
CVE-2026-3204	Improper input validation in the error message page in Devolutions Server 2025.3.15 and earlier allows remote attackers to spoof the displayed error message via a specially crafted URL.	N/A	More Details
CVE-2026-3224	Authentication bypass in the Microsoft Entra ID (Azure AD) authentication mode in Devolutions Server 2025.3.15.0 and earlier allows an unauthenticated user to authenticate as an arbitrary Entra ID user via a forged JSON Web Token (JWT).	N/A	More Details
CVE-2026-27601	Underscore.js is a utility-belt library for JavaScript. Prior to 1.13.8, the _.flatten and _.isEqual functions use recursion without a depth limit. Under very specific conditions, detailed below, an attacker could exploit this in a Denial of Service (DoS) attack by triggering a stack overflow. Untrusted input must be used to create a recursive datastructure, for example using JSON.parse, with no enforced depth limit. The datastructure thus created must be passed to _.flatten or _.isEqual. In the case of _.flatten, the vulnerability can only be exploited if it is possible for a remote client to prepare a datastructure that consists of arrays at all levels AND if no finite depth limit is passed as the second argument to _.flatten. In the case of _.isEqual, the vulnerability can only be exploited if there exists a code path in which two distinct datastructures that were submitted by the same remote client are compared using _.isEqual. For example, if a client submits data that are stored in a database, and the same client can later submit another datastructure that is then compared to the data that were saved in the database previously, OR if a client submits a single request, but its data are parsed twice, creating two non-identical but equivalent datastructures that are then compared. Exceptions originating from the call to _.flatten or _.isEqual, as a result of a stack overflow, are not being caught. This vulnerability is fixed in 1.13.8.	N/A	More Details
CVE-	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In CompositeDeepScanLine::readPixels, per-pixel totals are accumulated in vector<unsigned int> total_sizes for attacker-controlled large		

2026-27622	counts across many parts, total_sizes[ptr] wraps modulo 2^32. overall_sample_count is then derived from wrapped totals and used in samples[channel].resize(overall_sample_count). Decode pointer setup/consumption proceeds with true sample counts, and write operations in core unpack (generic_unpack_deep_pointers) overrun the undersized composite sample buffer. This vulnerability is fixed in v3.2.6, v3.3.8, and v3.4.6.	N/A	More Details
CVE-2026-27905	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.36, the safe_extract_tarfile() function validates that each tar member's path is within the destination directory, but for symlink members it only validates the symlink's own path, not the symlink's target. An attacker can create a malicious bento/model tar file containing a symlink pointing outside the extraction directory, followed by a regular file that writes through the symlink, achieving arbitrary file write on the host filesystem. This vulnerability is fixed in 1.4.36.	N/A	More Details
CVE-2026-27971	Qwik is a performance focused javascript framework. qwik <=1.19.0 is vulnerable to RCE due to an unsafe deserialization vulnerability in the server$ RPC mechanism that allows any unauthenticated user to execute arbitrary code on the server with a single HTTP request. Affects any deployment where require() is available at runtime. This vulnerability is fixed in 1.19.1.	N/A	More Details
CVE-2026-3076	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-2363. Reason: This candidate is a reservation duplicate of CVE-2026-2363. Notes: All CVE users should reference CVE-2026-2363 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-70237	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetPortTr.	N/A	More Details
CVE-2024-55026	An issue in the reset_pj.cgi endpoint of Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 allows unauthorized attackers to execute arbitrary commands via supplying a crafted GET request.	N/A	More Details
CVE-2025-66945	A path traversal vulnerability exists in the ZIP extraction API of Zdir Pro 4.x. When a crafted ZIP archive is processed by the backend at /api/extract, files may be written outside the intended directory, leading to arbitrary file overwrite and potentially remote code execution	N/A	More Details
CVE-2026-26886	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /admin/services/manage_service.php.	N/A	More Details
CVE-2025-57622	An issue in Step-Video-T2V allows a remote attacker to execute arbitrary code via the /vae-api , /caption-api , feature = pickle.loads(request.get_data()) component	N/A	More Details
CVE-2025-70821	renren-secuity before v5.5.0 is vulnerable to SQL Injection in the BaseServiceImpl.java component	N/A	More Details
CVE-2026-24103	A buffer overflow vulnerability was discovered in goform/formSetMacFilterCfg in Tenda AC15V1.0 V15.03.05.18_multi.	N/A	More Details
CVE-2026-2637	iBoysoft NTFS for Mac contains a local privilege escalation vulnerability in its privileged helper daemon ntfshelperd. The daemon exposes an NSConnection service that runs as root without implementing any authentication or authorization checks. This issue affects iBoysoft NTFS: 8.0.0.	N/A	More Details
CVE-2025-62814	An issue was discovered in Samsung Mobile Processor Exynos 1280, 2200, 1380, 1480, and 2400. A NULL pointer dereference of ft_handle in load_fw_utc_vector() causes a denial of service.	N/A	More Details
CVE-2025-62815	An issue was discovered in Samsung Mobile Processor Exynos 1380, 1480, 2400, 1580, and 2500. A NULL pointer dereference of npu_proto_drv.ast.thread_ref in set_cpu_affinity() causes a denial of service.	N/A	More Details
CVE-2025-66363	An issue was discovered in LBS in Samsung Mobile Processor Exynos 2200. There was no check for memory initialization within DL NAS Transport messages.	N/A	More Details

CVE-2025-66680	An issue in the WiseDelfile64.sys component of WiseCleaner Wise Force Deleter 7.3.2 and earlier allows attackers to delete arbitrary files via a crafted request.	N/A	More Details
CVE-2025-62816	An issue was discovered in Samsung Mobile Processor Exynos 1280, 2200, 1380, 1480, 2400, 1580, and 2500. Unvalidated VS4L_VERTEXIOC_BOOTUP input leads to a denial of service.	N/A	More Details
CVE-2025-62817	An issue was discovered in Samsung Mobile Processor Exynos 1280, 2200, 1380, 1480, 2400, 1580, and 2500. A NULL pointer dereference of session->ncp_hdr_buf in __pilot_parsing_ncp() causes a denial of service.	N/A	More Details
CVE-2026-3136	An improper authorization vulnerability in GitHub Trigger Comment Control in Google Cloud Build prior to 2026-1-26 allows a remote attacker to execute arbitrary code in the build environment. This vulnerability was patched on 26 January 2026, and no customer action is needed.	N/A	More Details
CVE-2024-55027	Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 was discovered to stroe credentials in plaintext in the component uac_temp.db.	N/A	More Details
CVE-2021-35483	The Applications component of Nokia IMPACT version through 19.11.2.10-20210118042150283 allows an authenticated user to arbitrarily upload JavaScript files via the /ui/rest-proxy/application fileupload parameter. This can occur during the adding of a new application, or during the editing of an existing one. If an authenticated user visits the web page where the file is published, the JavaScript code is executed.	N/A	More Details
CVE-2021-35484	Nokia IMPACT through 19.11.2.10-20210118042150283 allows an authenticated user to perform a Time-based Boolean Blind SQL Injection attack on the endpoint /ui/rest-proxy/campaign/statistic (for the View Campaign page) via the sortColumn HTTP GET parameter. This allows an attacker to access sensitive data from the database and obtain access to the database user, database name, and database version information.	N/A	More Details
CVE-2026-3343	A reflected cross-site scripting (XSS) vulnerability in the Fireware OS Web UI enabled execution of malicious JavaScript in the context of an authenticated management user's browser when they click on a specially crafted link. This vulnerability affects Fireware OS 12.7 up to and including 12.11.7 and 2025.1 up to and including 2026.1.1.	N/A	More Details
CVE-2021-35485	The Applications component of Nokia IMPACT version through 19.11.2.10-20210118042150283 allows an authenticated user to arbitrarily upload server-side executable files via the /ui/rest-proxy/application fileupload parameter. This can occur during the adding of a new application, or during the editing of an existing one.	N/A	More Details
CVE-2021-35486	A Cross-Site Request Forgery (CSRF) vulnerability in Nokia IMPACT through 19.11.2.10-20210118042150283 allows a remote attacker to import and overwrite the entire application configuration. Specifically, in /ui/rest-proxy/entity/import, neither the X-CSRF-NONCE HTTP header nor the CSRF-NONCE cookie is validated.	N/A	More Details
CVE-2026-1875	Improper Resource Shutdown or Release vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP all versions allows a remote attacker to cause a denial-of-service (DoS) condition on the products by continuously sending UDP packets to the products. A system reset of the product is required for recovery.	N/A	More Details
CVE-2025-63912	Cohesity TranZman Migration Appliance Release 4.0 Build 14614 was discovered to use a weak cryptography algorithm for data encryption, allowing attackers to trivially reverse the encyption and expose credentials.	N/A	More Details
CVE-2026-3437	An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Portwell Engineering Toolkits version 4.8.2 could allow a local authenticated attacker to read and write to arbitrary memory via the Portwell Engineering Toolkits driver. Successful exploitation of this vulnerability could result in escalation of privileges or cause a denial-of-service condition.	N/A	More Details
CVE-2024-55021	Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 was discovered to contain a hardcoded password in the FTP protocol.	N/A	More Details
CVE-	Weintek cMT-3072XH2 easyweb v2.1.53, OS v20231011 was discovered to contain an		More

2024-55022	authenticated command injection vulnerability via the HMI Name parameter.	N/A	Details
CVE-2026-1876	Improper Resource Shutdown or Release vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP all versions allows a remote attacker to cause a denial-of-service (DoS) condition on the products by continuously sending UDP packets to the products. A system reset of the product is required for recovery.	N/A	More Details
CVE-2026-1198	SIMPLE.ERP is vulnerable to the SQL Injection in search functionality in "Obroty na kontach" window. Lack of input validation allows an authenticated attacker to prepare a malicious query to the database that will be executed. This issue was fixed in 6.30@A04.4_u06.	N/A	More Details
CVE-2026-1874	Always-Incorrect Control Flow Implementation vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP versions 1.106 and prior and Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP all versions allows a remote attacker to cause a denial-of-service (DoS) condition on the products by continuously sending UDP packets to the products. A system reset of the product is required for recovery.	N/A	More Details
CVE-2026-27776	IM-LogicDesigner module of intra-mart Accel Platform contains insecure deserialization issue. This can be exploited only when IM-LogicDesigner is deployed on the system. Arbitrary code may be executed when some crafted file is imported by a user with the administrative privilege.	N/A	More Details
CVE-2026-24497	Stack-based Buffer Overflow vulnerability in SimTech Systems, Inc. ThinkWise allows Remote Code Inclusion.This issue affects ThinkWise: from 7 through 23.	N/A	More Details
CVE-2026-24498	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in EFM-Networks, Inc. IpTIME T5008, EFM-Networks, Inc. IpTIME AX2004M, EFM-Networks, Inc. IpTIME AX3000Q, EFM-Networks, Inc. IpTIME AX6000M allows Authentication Bypass.This issue affects ipTIME T5008: through 15.26.8; ipTIME AX2004M: through 15.26.8; ipTIME AX3000Q: through 15.26.8; ipTIME AX6000M: through 15.26.8.	N/A	More Details
CVE-2026-27735	Model Context Protocol Servers is a collection of reference implementations for the model context protocol (MCP). In mcp-server-git versions prior to 2026.1.14, the git_add tool did not validate that file paths provided in the files argument were within the repository boundaries. Because the tool used GitPython's repo.index.add() rather than the Git CLI, relative paths containing `../` sequences that resolve outside the repository were accepted and staged into the Git index. Users are advised to upgrade to 2026.1.14 or newer to remediate this issue.	N/A	More Details
CVE-2026-27613	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. A vulnerability in versions prior to 2.01 allows unauthenticated remote attackers to bypass the web server's CGI parameter security controls. Depending on the server configuration and the specific CGI executable in use, the impact is either source code disclosure or remote code execution (RCE). Anyone hosting CGI scripts (particularly interpreted languages like PHP) using vulnerable versions of TinyWeb is impacted. The problem has been patched in version 2.01. If upgrading is not immediately possible, ensure `STRICT_CGI_PARAMS` is enabled (it is defined by default in `define.inc`) and/or do not use CGI executables that natively accept dangerous command-line flags (such as `php-cgi.exe`). If hosting PHP, consider placing the server behind a Web Application Firewall (WAF) that explicitly blocks URL query string parameters that begin with a hyphen (`-`) or contain encoded double quotes (`%22`).	N/A	More Details
CVE-2026-27578	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could inject arbitrary scripts into pages rendered by the n8n application using different techniques on various nodes (Form Trigger node, Chat Trigger node, Send & Wait node, Webhook Node, and Chat Node). Scripts injected by a malicious workflow execute in the browser of any user who visits the affected page, enabling session hijacking and account takeover. The issues have been fixed in n8n versions 2.10.1 and 1.123.21. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Webhook node by adding `n8n-nodes-base.webhook` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, additional exploits in the expression evaluation of n8n have been identified and patched following		

CVE-2026-27577	CVE-2025-68613. An authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution on the host running n8n. The issues have been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate all known vulnerabilities. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or deploy n8n in a hardened environment with restricted operating system privileges and network access to reduce the impact of potential exploitation. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2026-27653	The installers for multiple products provided by Soliton Systems K.K. contain an issue with incorrect default permissions, which may allow arbitrary code to be executed with SYSTEM privileges.	N/A	More Details
CVE-2026-27498	n8n is an open source workflow automation platform. Prior to versions 2.2.0 and 1.123.8, an authenticated user with permission to create or modify workflows could chain the Read/Write Files from Disk node with git operations to achieve remote code execution. By writing to specific configuration files and then triggering a git operation, the attacker could execute arbitrary shell commands on the n8n host. The issue has been fixed in n8n versions 2.2.0 and 1.123.8. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Read/Write Files from Disk node by adding `n8n-nodes-base.readWriteFile` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2025-15509	The SmartRemote module has insufficient restrictions on loading URLs, which may lead to some information leakage.	N/A	More Details
CVE-2025-15567	Insufficient protection mechanisms in the Health Module may lead to partial information disclosure.	N/A	More Details
CVE-2026-27497	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could leverage the Merge node's SQL query mode to execute arbitrary code and write arbitrary files on the n8n server. The issues have been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate all known vulnerabilities. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Merge node by adding `n8n-nodes-base.merge` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2026-27495	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could exploit a vulnerability in the JavaScript Task Runner sandbox to execute arbitrary code outside the sandbox boundary. On instances using internal Task Runners (default runner mode), this could result in full compromise of the n8n host. On instances using external Task Runners, the attacker might gain access to or impact other task executed on the Task Runner. Task Runners must be enabled using `N8N_RUNNERS_ENABLED=true`. The issue has been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or use external runner mode (`N8N_RUNNERS_MODE=external`) to limit the blast radius. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2026-27812	Sub2API is an AI API gateway platform designed to distribute and manage API quotas from AI product subscriptions. A vulnerability in versions prior to 0.1.85 is a Password Reset Poisoning (Host Header / Forwarded Header trust issue), which allows attackers to manipulate the password reset link. Attackers can exploit this flaw to inject their own domain into the password reset link, leading to the potential for account takeover. The vulnerability has been fixed in version v0.1.85. If upgrading is not immediately possible, users can mitigate the vulnerability by disabling the	N/A	More Details

	"forgot password" feature until an upgrade to a patched version can be performed. This will prevent attackers from exploiting the vulnerability via the affected endpoint.		
CVE-2026-27494	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could use the Python Code node to escape the sandbox. The sandbox did not sufficiently restrict access to certain built-in Python objects, allowing an attacker to exfiltrate file contents or achieve RCE. On instances using internal Task Runners (default runner mode), this could result in full compromise of the n8n host. On instances using external Task Runners, the attacker might gain access to or impact other task executed on the Task Runner. Task Runners must be enabled using `N8N_RUNNERS_ENABLED=true`. The issue has been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to this version or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only., and/or disable the Code node by adding `n8n-nodes-base.code` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2025-15498	Pro3W CMS if vulnerable to SQL injection attacks. Improper neutralization of input provided into a login form allows an unauthenticated attacker to bypass authentication and gain administrative privileges. This issue was identified in version 1.2.0 of this software. Due to lack of response from the vendor exact version range could not be determined, but the vulnerability should be eliminated in versions released in January 2026 and later.	N/A	More Details
CVE-2026-27493	n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, a second-order expression injection vulnerability existed in n8n's Form nodes that could allow an unauthenticated attacker to inject and evaluate arbitrary n8n expressions by submitting crafted form data. When chained with an expression sandbox escape, this could escalate to remote code execution on the n8n host. The vulnerability requires a specific workflow configuration to be exploitable. First, a form node with a field interpolating a value provided by an unauthenticated user, e.g. a form submitted value. Second, the field value must begin with an `=` character, which caused n8n to treat it as an expression and triggered a double-evaluation of the field content. There is no practical reason for a workflow designer to prefix a field with `=` intentionally — the character is not rendered in the output, so the result would not match the designer's expectations. If added accidentally, it would be noticeable and very unlikely to persist. An unauthenticated attacker would need to either know about this specific circumstance on a target instance or discover a matching form by chance. Even when the preconditions are met, the expression injection alone is limited to data accessible within the n8n expression context. Escalation to remote code execution requires chaining with a separate sandbox escape vulnerability. The issue has been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Review usage of form nodes manually for above mentioned preconditions, disable the Form node by adding `n8n-nodes-base.form` to the `NODES_EXCLUDE` environment variable, and/or disable the Form Trigger node by adding `n8n-nodes-base.formTrigger` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	N/A	More Details
CVE-2026-3223	Arbitrary file write & potential privilege escalation exploiting zip slip vulnerability in Google Web Designer.	N/A	More Details
CVE-2026-3327	Authenticated Iframe Injection in Dato CMS Web Previews plugin. This vulnerability permits a malicious authenticated user to circumvent the restriction enforced on the configured frontend URL, enabling the loading of arbitrary external resources or origins. This issue affects Web Previews < v1.0.31.	N/A	More Details
CVE-2026-2359	Multer is a node.js middleware for handling `multipart/form-data`. A vulnerability in Multer prior to version 2.1.0 allows an attacker to trigger a Denial of Service (DoS) by dropping connection during file upload, potentially causing resource exhaustion. Users should upgrade to version 2.1.0 to receive a patch. No known workarounds are available.	N/A	More Details
CVE-2026-3277	The OpenID Connect (OIDC) authentication configuration in PowerShell Universal before 2026.1.3 stores the OIDC client secret in cleartext in the .universal/authentication.ps1 script, which allows an attacker with read access to that file to obtain the OIDC client credentials	N/A	More Details

CVE-2026-3304	Multer is a node.js middleware for handling `multipart/form-data`. A vulnerability in Multer prior to version 2.1.0 allows an attacker to trigger a Denial of Service (DoS) by sending malformed requests, potentially causing resource exhaustion. Users should upgrade to version 2.1.0 to receive a patch. No known workarounds are available.	N/A	More Details
CVE-2026-2293	A NestJS application using @nestjs/platform-fastify can allow bypass of authentication/authorization middleware when Fastify path-normalization options are enabled. This issue affects nest.Js: 11.1.13.	N/A	More Details
CVE-2026-27148	Storybook is a frontend workshop for building user interface components and pages in isolation. Prior to versions 7.6.23, 8.6.17, 9.1.19, and 10.2.10, the WebSocket functionality in Storybook's dev server, used to create and update stories, is vulnerable to WebSocket hijacking. This vulnerability only affects the Storybook dev server; production builds are not impacted. Exploitation requires a developer to visit a malicious website while their local Storybook dev server is running. Because the WebSocket connection does not validate the origin of incoming connections, a malicious site can silently send WebSocket messages to the local instance without any further user interaction. If the Storybook dev server is intentionally exposed publicly (e.g. for design reviews or stakeholder demos) the risk is higher, as no malicious site visit is required. Any unauthenticated attacker can send WebSocket messages to it directly. The vulnerability affects the WebSocket message handlers for creating and saving stories. Both are vulnerable to injection via unsanitized input in the componentFilePath field, which can be exploited to achieve persistent XSS or Remote Code Execution (RCE). Versions 7.6.23, 8.6.17, 9.1.19, and 10.2.10 contain a fix for the issue.	N/A	More Details
CVE-2026-26984	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. Prior to versions 26.0.5, 27.0.2, and 28.0.0, an authenticated user with sufficient privileges can exploit a path traversal vulnerability to upload a malicious file to an arbitrary location on the server. Once uploaded, the file can be used to achieve remote code execution (RCE). An attacker must be authenticated and have the appropriate permissions to exploit this issue. If the server is configured as read-only, remote code execution (RCE) is not possible; however, the malicious file upload may still be achievable. This problem is fixed in LORIS v26.0.5 and above, v27.0.2 and above, and v28.0.0 and above. As a workaround, LORIS administrators can disable the media module if it is not being used.	N/A	More Details
CVE-2026-27804	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.3 and 9.1.1-alpha.4, an unauthenticated attacker can forge a Google authentication token with `alg: "none"` to log in as any user linked to a Google account, without knowing their credentials. All deployments with Google authentication enabled are affected. The fix in versions 8.6.3 and 9.1.1-alpha.4 hardcodes the expected `RS256` algorithm instead of trusting the JWT header, and replaces the Google adapter's custom key fetcher with `jwks-rsa` which rejects unknown key IDs. As a workaround, dsable Google authentication until upgrading is possible.	N/A	More Details
CVE-2026-27818	TerriaJS-Server is a NodeJS Express server for TerriaJS, a library for building web-based geospatial data explorers. A validation bug in versions prior to 4.0.3 allows an attacker to proxy domains not explicitly allowed in the `proxyableDomains` configuration. Version 4.0.3 fixes the issue.	N/A	More Details
CVE-2026-2880	A vulnerability in @fastify/middie versions < 9.2.0 can result in authentication/authorization bypass when using path-scoped middleware (for example, app.use('/secret', auth)). When Fastify router normalization options are enabled (such as ignoreDuplicateSlashes, useSemicolonDelimiter, and related trailing-slash behavior), crafted request paths may bypass middleware checks while still being routed to protected handlers.	N/A	More Details
CVE-2026-1694	HTTP headers are added by the default configuration of IIS and ASP.net, and are not removed at the deployment phase of the webservices used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It unnecessarily exposes sensitive information about the server configuration.	N/A	More Details
CVE-2026-2244	A vulnerability in Google Cloud Vertex AI Workbench from 7/21/2025 to 01/30/2026 allows an attacker to exfiltrate valid Google Cloud access tokens of other users via abuse of a built-in startup script. All instances after January 30th, 2026 have been patched to protect from this vulnerability. No user action is required for this.	N/A	More Details
CVE-	A HTTP Host header attack vulnerability affects WebClient and the WebScheduler web apps of PcVue in version 15.0.0 through 16.3.3 included, allowing a remote attacker to inject harmful		

2026-1698	payloads that manipulate server-side behavior. This vulnerability only affects the endpoints /Authentication/ExternalLogin, /Authentication/AuthorizationCodeCallback and /Authentication/Logout of the WebClient and WebScheduler web apps.	N/A	More Details
CVE-2026-1697	The Secure and SameSite attribute are missing in the GraphicalData web services and WebClient web app of PcVue in version 12.0.0 through 16.3.3 included.	N/A	More Details
CVE-2026-1696	Some HTTP security headers are not properly set by the web server when sending responses to the client application.	N/A	More Details
CVE-2025-11381	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11382	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11383	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11384	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-1241	The Pelco, Inc. Sarix Professional 3 Series Cameras are vulnerable to an authentication bypass issue in their web management interface. The flaw stems from inadequate enforcement of access controls, allowing certain functionality to be accessed without proper authentication. This weakness can lead to unauthorized viewing of live video streams, creating privacy concerns and operational risks for organizations relying on these cameras. Additionally, it may expose operators to regulatory and compliance challenges.	N/A	More Details
CVE-2026-1695	An XSS vulnerability affects the OAuth web services used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It might allow a remote attacker to trick a legitimate user into loading content from another site upon unsuccessful user authentication on an unknown application (unknown client_id). This vulnerability only affects the error page of the OAuth server.	N/A	More Details
CVE-2026-23939	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in hexpm hexpm/hexpm ('Elixir.Hexpm.Store.Local' module) allows Relative Path Traversal. This vulnerability is associated with program files lib/hexpm/store/local.ex and program routines 'Elixir.Hexpm.Store.Local':get/3, 'Elixir.Hexpm.Store.Local':put/4, 'Elixir.Hexpm.Store.Local':delete/2, 'Elixir.Hexpm.Store.Local':delete_many/2. This issue does NOT affect hex.pm the service. Only self-hosted deployments using the Local Storage backend are affected. This issue affects hexpm: from 931ee0ed46fa89218e0400a4f6e6d15f96406050 before 5d2ccd2f14f45a63225a73fb5b1c937baf36fdc0.	N/A	More Details
CVE-2026-1693	The OAuth grant type Resource Owner Password Credentials (ROPC) flow is still used by the werbservices used by the WebVue, WebScheduler, TouchVue and Snapvue features of PcVue in version 12.0.0 through 16.3.3 included despite being deprecated. It might allow a remote attacker to steal user credentials.	N/A	More Details
CVE-2026-27821	GPAC is an open-source multimedia framework. In versions up to and including 26.02.0, a stack buffer overflow occurs during NHML file parsing in `src/filters/dmx_nhml.c`. The value of the xmlHeaderEnd XML attribute is copied from att->value into szXmlHeaderEnd[1000] using strcpy() without any length validation. If the input exceeds 1000 bytes, it overwrites beyond the stack buffer boundary. Commit 9bd7137fded2db40de61a2cf3045812c8741ec52 patches the issue.	N/A	More Details
CVE-2023-31364	Improper handling of direct memory writes in the input-output memory management unit could allow a malicious guest virtual machine (VM) to flood a host with writes, potentially causing a fatal machine check error resulting in denial of service.	N/A	More Details
	A missing origin validation in WebSockets vulnerability affects the GraphicalData web services		

CVE-2026-1692	used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It might allow a remote attacker to lure a successfully authenticated user to a malicious website. This vulnerability only affects the following two endpoints: GraphicalData/js/signalR/connect and GraphicalData/js/signalR/reconnect.	N/A	More Details
CVE-2026-25191	The installer of FinalCode Client provided by Digital Arts Inc. contains an issue with the DLL search path. If a user is directed to place a malicious DLL file and the installer to the same directory and execute the installer, arbitrary code may be executed with the installer's execution privilege.	N/A	More Details
CVE-2026-23703	The installer of FinalCode Client provided by Digital Arts Inc. contains an incorrect default permissions vulnerability. A non-administrative user may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2026-27902	Svelte performance oriented web framework. Prior to version 5.53.5, errors from `transformError` were not correctly escaped prior to being embedded in the HTML output, causing potential HTML injection and XSS if attacker-controlled content is returned from `transformError`. Version 5.53.5 fixes the issue.	N/A	More Details
CVE-2026-27901	Svelte performance oriented web framework. Prior to version 5.53.5, the contents of `bind:innerText` and `bind:textContent` on `contenteditable` elements were not properly escaped. This could enable HTML injection and Cross-Site Scripting (XSS) if rendering untrusted data as the binding's initial value on the server. Version 5.53.5 fixes the issue.	N/A	More Details
CVE-2026-27887	Spin is an open source developer tool for building and running serverless applications powered by WebAssembly. When Spin is configured to allow connections to a database or web server which could return responses of unbounded size (e.g. tables with many rows or large content bodies), Spin may in some cases attempt to buffer the entire response before delivering it to the guest, which can lead to the host process running out of memory, panicking, and crashing. In addition, a malicious guest application could incrementally insert a large number of rows or values into a database and then retrieve them all in a single query, leading to large host allocations. Spin 3.6.1, SpinKube 0.6.2, and `containerd-shim-spin` 0.22.1 have been patched to address the issue. As a workaround, configure Spin to only allow access to trusted databases and HTTP servers which limit response sizes.	N/A	More Details
CVE-2026-27946	ZITADEL is an open source identity management platform. Prior to versions 4.11.1 and 3.4.7, a vulnerability in Zitadel's self-management capability allowed users to mark their email and phone as verified without going through an actual verification process. The patch in versions 4.11.1 and 3.4.7 resolves the issue by requiring the correct permission in case the verification flag is provided and only allows self-management of the email address and/or phone number itself. If an upgrade is not possible, an action (v2) could be used to prevent setting the verification flag on the own user.	N/A	More Details
CVE-2026-27945	ZITADEL is an open source identity management platform. Zitadel Action V2 (introduced as early preview in 2.59.0, beta in 3.0.0 and GA in 4.0.0) is a webhook based approach to allow developers act on API request to Zitadel and customize flows such the issue of a token. Zitadel's Action target URLs can point to local hosts, potentially allowing adversaries to gather internal network information and connect to internal services. When the URL points to a local host / IP address, an adversary might gather information about the internal network structure, the services exposed on internal hosts etc. This is sometimes called a Server-Side Request Forgery (SSRF). Zitadel Actions expect responses according to specific schemas, which reduces the threat vector. The patch in version 4.11.1 resolves the issue by checking the target URL against a denylist. By default localhost, resp. loopback IPs are denied. Note that this fix was only released on v4.x. Due to the stage (preview / beta) in which the functionality was in v2.x and v3.x, the changes that have been applied to it since then and the severity, respectively the actual thread vector, a backport to the corresponding versions was not feasible. Please check the workaround section for alternative solutions if an upgrade to v4.x is not possible. If an upgrade is not possible, prevent actions from using unintended endpoints by setting network policies or firewall rules in one's own infrastructure. Note that this is outside of the functionality provided by Zitadel.	N/A	More Details
CVE-2026-27896	The Go MCP SDK used Go's standard encoding/json.Unmarshal for JSON-RPC and MCP protocol message parsing in versions prior to 1.3.1. Go's standard library performs case-insensitive matching of JSON keys to struct field tags — a field tagged json:"method" would also match "Method", "METHOD", etc. This violated the JSON-RPC 2.0 specification, which defines exact field names. A malicious MCP peer may have been able to send protocol messages with non-standard field casing that the SDK would silently accept. This had the potential for bypassing intermediary inspection and coss-implementation inconsistency. Go's standard JSON unmarshaling was	N/A	More Details

	replaced with a case-sensitive decoder in commit 7b8d81c. Users are advised to update to v1.3.1 to resolve this issue.		
CVE-2026-27830	c3p0, a JDBC Connection pooling library, is vulnerable to attack via maliciously crafted Java-serialized objects and `javax.naming.Reference` instances. Several c3p0 `ConnectionPoolDataSource` implementations have a property called `userOverridesAsString` which conceptually represents a `Map<String,Map<String,String>>`. Prior to v0.12.0, that property was maintained as a hex-encoded serialized object. Any attacker able to reset this property, on an existing `ConnectionPoolDataSource` or via maliciously crafted serialized objects or `javax.naming.Reference` instances could be tailored execute unexpected code on the application's `CLASSPATH`. The danger of this vulnerability was strongly magnified by vulnerabilities in c3p0's main dependency, mchange-commons-java. This library includes code that mirrors early implementations of JNDI functionality, including ungated support for remote `factoryClassLocation` values. Attackers could set c3p0's `userOverridesAsString` hex-encoded serialized objects that include objects "indirectly serialized" via JNDI references. Deserialization of those objects and dereferencing of the embedded `javax.naming.Reference` objects could provoke download and execution of malicious code from a remote `factoryClassLocation`. Although hazard presented by c3p0's vulnerabilites are exarcerbated by vulnerabilities in mchange-commons-java, use of Java-serialized-object hex as the format for a writable Java-Bean property, of objects that may be exposed across JNDI interfaces, represents a serious independent fragility. The `userOverridesAsString` property of c3p0 `ConnectionPoolDataSource` classes has been reimplemented to use a safe CSV-based format, rather than rely upon potentially dangerous Java object deserialization. c3p0-0.12.0+ and above depend upon mchange-commons-java 0.4.0+, which gates support for remote `factoryClassLocation` values by configuration parameters that default to restrictive values. c3p0 additionally enforces the new mchange-commons-java `com.mchange.v2.naming.nameGuardClassName` to prevent injection of unexpected, potentially remote JNDI names. There is no supported workaround for versions of c3p0 prior to 0.12.0.	N/A	More Details
CVE-2026-21619	Uncontrolled Resource Consumption, Deserialization of Untrusted Data vulnerability in hexpm hex_core (hex_api modules), hexpm hex (mix_hex_api modules), erlang rebar3 (r3_hex_api modules) allows Object Injection, Excessive Allocation. This vulnerability is associated with program files src/hex_api.erl, src/mix_hex_api.erl, apps/rebar/src/vendored/r3_hex_api.erl and program routines hex_core:request/4, mix_hex_api:request/4, r3_hex_api:request/4. This issue affects hex_core: from 0.1.0 before 0.12.1; hex: from 2.3.0 before 2.3.2; rebar3: from 3.9.1 before 3.27.0.	N/A	More Details
CVE-2026-27200	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2025-15595	Privilege escalation via dll hijacking in Inno Setup 6.2.1 and ealier versions.	N/A	More Details
CVE-2026-27701	LiveCode is an open-source, client-side code playground. Prior to commit e151c64c2bd80d2d53ac1333f1df9429fe6a1a11, LiveCode's `i18n-update-pull` GitHub Actions workflow is vulnerable to JavaScript injection. The title of the Pull Request associated with the triggering issue comment is interpolated directly into a `actions/github-script` JavaScript block using a GitHub Actions template expression. An attacker who opens a PR with a crafted title can inject arbitrary JavaScript that executes with the privileges of the CI bot token (`CI_APP_ID` / `CI_APP_PRIVATE_KEY`), enabling exfiltration of repository secrets and unauthorized GitHub API operations. Commit e151c64c2bd80d2d53ac1333f1df9429fe6a1a11 fixes the issue.	N/A	More Details
CVE-2025-58402	The CGM CLININET application uses direct, sequential object identifiers "MessageID" without proper authorization checks. By modifying the parameter in the GET request, an attacker can access messages and attachments belonging to other users.	N/A	More Details
CVE-2025-58405	The CGM CLININET application does not implement any mechanisms that prevent clickjacking attacks, neither HTTP security headers nor HTML-based frame-busting protections were detected. As a result, an attacker can embed the application inside a maliciously crafted IFRAME and trick users into performing unintended actions, including potentially bypassing CSRF/XSRF defenses.	N/A	More Details
CVE-2025-58406	The CGM CLININET application respond without essential security HTTP headers, exposing users to client-side attacks such as clickjacking, MIME sniffing, unsafe caching, weak cross-origin isolation, and missing transport security controls.	N/A	More Details

CVE-2025-12462	A Blind SQL injection vulnerability has been identified in DobryCMS. A remote unauthenticated attacker is able to inject SQL syntax into URL path resulting in Blind SQL Injection. This issue was fixed in versions above 8.0.	N/A	More Details
CVE-2025-14532	DobryCMS's upload file functionality allows an unauthenticated remote attacker to upload files of any type and extension without restriction, which can result in Remote Code Execution. This issue was fixed in versions above 5.0.	N/A	More Details
CVE-2026-3432	On SimStudio version below to 0.5.74, the `/api/auth/oauth/token` endpoint contains a code path that bypasses all authorization checks when provided with `credentialAccountUserId` and `providerId` parameters. An unauthenticated attacker can retrieve OAuth access tokens for any user by supplying their user ID and a provider name, effectively stealing credentials to third-party services.	N/A	More Details
CVE-2026-27727	mchange-commons-java, a library that provides Java utilities, includes code that mirrors early implementations of JNDI functionality, including support for remote `factoryClassLocation` values, by which code can be downloaded and invoked within a running application. If an attacker can provoke an application to read a maliciously crafted `jaxax.naming.Reference` or serialized object, they can provoke the download and execution of malicious code. Implementations of this functionality within the JDK were disabled by default behind a System property that defaults to `false`, `com.sun.jndi.ldap.object.trustURLCodebase`. However, since mchange-commons-java includes an independent implementation of JNDI derefencing, libraries (such as c3p0) that resolve references via that implementation could be provoked to download and execute malicious code even after the JDK was hardened. Mirroring the JDK patch, mchange-commons-java's JNDI functionality is gated by configuration parameters that default to restrictive values starting in version 0.4.0. No known workarounds are available. Versions prior to 0.4.0 should be avoided on application CLASSPATHs.	N/A	More Details
CVE-2026-23600	A remote authentication bypass vulnerability exists in HPE AutoPass License Server (APLS).	N/A	More Details
CVE-2026-0689	In ExtremeCloud IQ – Site Engine (XIQ-SE) before 26.2.10, a vulnerability in the NAC administration interface allows an authenticated NAC administrator to retrieve masked sensitive parameters from HTTP responses. Although credentials appear redacted in the user interface, the application returns the underlying credential values in the HTTP response, enabling an authorized administrator to recover stored secrets that may exceed their intended access. We would like to thank the Lockheed Martin Red Team for responsibly reporting this issue and working with us through coordinated disclosure.	N/A	More Details
CVE-2026-3206	Improper Resource Shutdown or Release vulnerability in KrakenD, SLU KrakenD-CE (CircuitBreaker modules), KrakenD, SLU KrakenD-EE (CircuitBreaker modules). This issue affects KrakenD-CE: before 2.13.1; KrakenD-EE: before 2.12.5.	N/A	More Details
CVE-2026-27704	The Dart and Flutter SDKs provide software development kits for the Dart programming language. In versions of the Dart SDK prior to 3.11.0 and the Flutter SDK prior to version 3.41.0, when the pub client (`dart pub` and `flutter pub`) extracts a package in the pub cache, a malicious package archive can have files extracted outside the destination directory in the `PUB_CACHE`. A fix has been landed in commit 26c6985c742593d081f8b58450f463a584a4203a. By normalizing the file path before writing file, the attacker can no longer traverse up via a symlink. This patch is released in Dart 3.11.0 and Flutter 3.41.0.vAll packages on pub.dev have been vetted for this vulnerability. New packages are no longer allowed to contain symlinks. The pub client itself doesn't upload symlinks, but duplicates the linked entry, and has been doing this for years. Those whose dependencies are all from pub.dev, third-party repositories trusted to not contain malicious code, or git dependencies are not affected by this vulnerability.	N/A	More Details
CVE-2026-22866	Ethereum Name Service (ENS) is a distributed, open, and extensible naming system based on the Ethereum blockchain. In versions 1.6.2 and prior, the `RSASHA256Algorithm` and `RSASHA1Algorithm` contracts fail to validate PKCS#1 v1.5 padding structure when verifying RSA signatures. The contracts only check if the last 32 (or 20) bytes of the decrypted signature match the expected hash. This enables Bleichenbacher's 2006 signature forgery attack against DNS zones using RSA keys with low public exponents (e=3). Two ENS-supported TLDs (.cc and .name) use e=3 for their Key Signing Keys, allowing any domain under these TLDs to be fraudulently claimed on ENS without DNS ownership. Apatch was merged at commit c76c5ad0dc9de1c966443bd946fafc6351f87587. Possible workarounds include deploying the	N/A	More Details

	patched contracts and pointing DNSSECImpl.setAlgorithm to the deployed contract.		
CVE-2025-30044	In the endpoints "/cgi-bin/CliniNET.prd/utils/usrlogstat_simple.pl", "/cgi-bin/CliniNET.prd/utils/usrlogstat.pl", "/cgi-bin/CliniNET.prd/utils/userlogstat2.pl", and "/cgi-bin/CliniNET.prd/utils/dblogstat.pl", the parameters are not sufficiently normalized, which enables code injection.	N/A	More Details
CVE-2026-3197	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-2026-0654	Improper input handling in the administration web interface on TP-Link Deco BE25 v1.0 allows crafted input to be executed as part of an OS command. An authenticated adjacent attacker may execute arbitrary commands via crafted configuration file, impacting confidentiality, integrity and availability of the device. This issue affects Deco BE25 v1.0: through 1.1.1 Build 20250822.	N/A	More Details
CVE-2026-0655	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TP-Link Deco BE25 v1.0 (web modules) allows authenticated adjacent attacker to read arbitrary files or cause denial of service. This issue affects Deco BE25 v1.0: through 1.1.1 Build 20250822.	N/A	More Details
CVE-2026-25701	An Insecure Temporary File vulnerability in openSUSE sdbootutil allows local users to pre-create a directory to achieve various effects like: * gain access to possible private information found in /var/lib/pcrlock.d * manipulate the data backed up in /tmp/pcrlock.d.bak, therefore violating the integrity of the data should it be restored. * overwrite protected system files with data from /var/lib/pcrlock.d by placing symlinks to existing files in the directory tree in /tmp/pcrlock.d.bak. This issue affects sdbootutil: from ? before 5880246d3a02642dc68f5c8cb474bf63cdb56bca.	N/A	More Details
CVE-2026-25785	Path traversal vulnerability exists in Lanscope Endpoint Manager (On-Premises) Sub-Manager Server Ver.9.4.7.3 and earlier, which may allow an attacker to tamper with arbitrary files and execute arbitrary code on the affected system.	N/A	More Details
CVE-2026-26709	code-projects Simple Gym Management System v1.0 is vulnerable to SQL Injection in /gym/trainer_search.php.	N/A	More Details
CVE-2026-25477	AFFiNE is an open-source, all-in-one workspace and an operating system. Prior to version 0.26.0, there is an Open Redirect vulnerability located at the /redirect-proxy endpoint. The flaw exists in the domain validation logic, where an improperly anchored Regular Expression allows an attacker to bypass the whitelist by using malicious domains that end with a trusted string. This issue has been patched in version 0.26.0.	N/A	More Details
CVE-2026-25884	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. Prior to version 0.28.8, an out-of-bounds read was found. The vulnerability is in the CRW image parser. This issue has been patched in version 0.28.8.	N/A	More Details
CVE-2026-27596	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. Prior to version 0.28.8, an out-of-bounds read was found in Exiv2. The vulnerability is in the preview component, which is only triggered when running Exiv2 with an extra command line argument, like -pp. The out-of-bounds read is at a 4GB offset, which usually causes Exiv2 to crash. This issue has been patched in version 0.28.8.	N/A	More Details
CVE-2026-27631	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. Prior to version 0.28.8, an uncaught exception was found in Exiv2. The vulnerability is in the preview component, which is only triggered when running Exiv2 with an extra command line argument, like -pp. Due to an integer overflow, the code attempts to create a huge std::vector, which causes Exiv2 to crash with an uncaught exception. This issue has been patched in version 0.28.8.	N/A	More Details
CVE-2026-0754	An embedded test key and certificate could be extracted from a Poly Voice device using specialized reverse engineering tools. This extracted certificate could be accepted by a SIP service provider if the service provider does not perform proper validation of the device certificate.	N/A	More Details
CVE-2025-30062	In the "CheckUnitCodeAndKey.pl" service, the "validateOrgUnit" function is vulnerable to SQL injection.	N/A	More Details

CVE-2025-30042	The CGM CLININET system provides smart card authentication; however, authentication is conducted locally on the client device, and, in reality, only the certificate number is used for access verification. As a result, possession of the certificate number alone is sufficient for authentication, regardless of the actual presence of the smart card or ownership of the private key.	N/A	More Details
CVE-2026-27201	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-28288	Dify is an open-source LLM app development platform. Prior to 1.9.0, responses from the Dify API to existing and non-existent accounts differ, allowing an attacker to enumerate email addresses registered with Dify. Version 1.9.0 fixes the issue.	N/A	More Details
CVE-2026-27500	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27501	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27573	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27580	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27581	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27582	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27583	Rejected reason: Further research determined the situation described is not a vulnerability.	N/A	More Details
CVE-2026-27832	Group-Office is an enterprise customer relationship management and groupware tool. Versions prior to 26.0.8, 25.0.87, and 6.8.153 have a SQL Injection (SQLi) vulnerability, exploitable through the `advancedQueryData` parameter (`comparator` field) on an authenticated endpoint. The endpoint `index.php?r=email/template/emailSelection` processes `advancedQueryData` and forwards the SQL comparator without a strict allowlist into SQL condition building. This enables blind boolean-based exfiltration of the `core_auth_password` table. Versions 26.0.8, 25.0.87, and 6.8.153 fix the issue.	N/A	More Details
CVE-2026-27947	Group-Office is an enterprise customer relationship management and groupware tool. Versions prior to 26.0.9, 25.0.87, and 6.8.154 have an authenticated Remote Code Execution vulnerability in the TNEF attachment processing flow. The vulnerable path extracts attacker-controlled files from `winmail.dat` and then invokes `zip` with a shell wildcard (`*`). Because extracted filenames are attacker-controlled, they can be interpreted as `zip` options and lead to arbitrary command execution. Versions 26.0.9, 25.0.87, and 6.8.154 fix the issue.	N/A	More Details
CVE-2026-28231	pillow_heif is a Python library for working with HEIF images and plugin for Pillow. Prior to version 1.3.0, an integer overflow in the encode path buffer validation of `_pillow_heif.c` allows an attacker to bypass bounds checks by providing large image dimensions, resulting in a heap out-of-bounds read. This can lead to information disclosure (server heap memory leaking into encoded images) or denial of service (process crash). No special configuration is required — this triggers under default settings. Version 1.3.0 fixes the issue.	N/A	More Details
	ServiceNow has addressed a remote code execution vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute code within the ServiceNow Sandbox. ServiceNow addressed this		

CVE-2026-0542	vulnerability by deploying a security update to hosted instances. Relevant security updates also have been provided to ServiceNow self-hosted customers and partners. Further, the vulnerability is addressed in the listed patches and hot fixes. While we are not currently aware of exploitation against customer instances, we recommend customers promptly apply appropriate updates or upgrade if they have not already done so.	N/A	More Details
CVE-2026-28355	Canarytokens help track activity and actions on a network. Versions prior to `sha-7ff0e12` have a Self Cross-Site Scripting vulnerability in the "PWA" Canarytoken, whereby the Canarytoken's creator can attack themselves or someone they share the link with. The creator of a PWA Canarytoken can insert Javascript into the title field of their PWA token. When the creator later browses the installation page for their own Canarytoken, the Javascript executes. This is a self-XSS. An attacker could create a Canarytoken with this self-XSS, and send the install link to a victim. When they click on it, the Javascript would execute. However, no sensitive information (ex. session information) will be disclosed to the malicious actor. This issue is now patched on Canarytokens.org. Users of self-hosted Canarytokens installations can update by pulling the latest Docker image, or any Docker image after sha-7ff0e12.	N/A	More Details
CVE-2025-30035	The vulnerability enables an attacker to fully bypass authentication in CGM CLININET and gain access to any active user account by supplying only the username, without requiring a password or any other credentials. Obtaining a session ID is sufficient for session takeover and grants access to the system with the privileges of the targeted user.	N/A	More Details
CVE-2026-27759	Featured Image from Content (featured-image-from-content) WordPress plugin versions prior to 1.7 contain an authenticated server-side request forgery vulnerability that allows Author-level users to fetch internal HTTP resources. Attackers can exploit insecure URL fetching and file write operations to retrieve sensitive internal data and store it in web-accessible upload directories.	N/A	More Details
CVE-2026-28515	openDCIM version 23.04, through commit 4467e9c4, contains a missing authorization vulnerability in install.php and container-install.php. The installer and upgrade handler expose LDAP configuration functionality without enforcing application role checks. Any authenticated user can access this functionality regardless of assigned privileges. In deployments where REMOTE_USER is set without authentication enforcement, the endpoint may be accessible without credentials. This allows unauthorized modification of application configuration.	N/A	More Details
CVE-2026-28516	openDCIM version 23.04, through commit 4467e9c4, contains a SQL injection vulnerability in Config::UpdateParameter. The install.php and container-install.php handlers pass user-supplied input directly into SQL statements using string interpolation without prepared statements or proper input sanitation. An authenticated user can execute arbitrary SQL statements against the underlying database.	N/A	More Details
CVE-2026-28517	openDCIM version 23.04, through commit 4467e9c4, contains an OS command injection vulnerability in report_network_map.php. The application retrieves the 'dot' configuration parameter from the database and passes it directly to exec() without validation or sanitation. If an attacker can modify the fac_Config.dot value, arbitrary commands may be executed in the context of the web server process.	N/A	More Details
CVE-2026-2647	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-2844	Missing Authentication for Critical Function vulnerability in Microchip TimePictra allows Configuration/Environment Manipulation.This issue affects TimePictra: from 11.0 through 11.3 SP2.	N/A	More Details
CVE-2026-3010	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Microchip TimePictra allows Query System for Information.This issue affects TimePictra: from 11.0 through 11.3 SP2.	N/A	More Details
	The Angular SSR is a server-rise rendering tool for Angular applications. Versions prior to 21.2.0-rc.1, 21.1.5, 20.3.17, and 19.2.21 have a Server-Side Request Forgery (SSRF) vulnerability in the Angular SSR request handling pipeline. The vulnerability exists because Angular’s internal URL reconstruction logic directly trusts and consumes user-controlled HTTP headers specifically the Host and `X-Forwarded-*` family to determine the application's base origin without any validation of the destination domain. Specifically, the framework didn't have checks for the host domain, path and character sanitization, and port validation. This vulnerability manifests in two primary		

CVE-2026-27739	ways: implicit relative URL resolution and explicit manual construction. When successfully exploited, this vulnerability allows for arbitrary internal request steering. This can lead to credential exfiltration, internal network probing, and a confidentiality breach. In order to be vulnerable, the victim application must use Angular SSR (Server-Side Rendering), the application must perform `HttpClient` requests using relative URLs OR manually construct URLs using the unvalidated `Host` / `X-Forwarded-*` headers using the `REQUEST` object, the application server must be reachable by an attacker who can influence these headers without strict validation from a front-facing proxy, and the infrastructure (Cloud, CDN, or Load Balancer) must not sanitize or validate incoming headers. Versions 21.2.0-rc.1, 21.1.5, 20.3.17, and 19.2.21 contain a patch. Some workarounds are available. Avoid using `req.headers` for URL construction. Instead, use trusted variables for base API paths. Those who cannot upgrade immediately should implement a middleware in their `server.ts` to enforce numeric ports and validated hostnames.	N/A	More Details
CVE-2026-27738	The Angular SSR is a server-rise rendering tool for Angular applications. An Open Redirect vulnerability exists in the internal URL processing logic in versions on the 19.x branch prior to 19.2.21, the 20.x branch prior to 20.3.17, and the 21.x branch prior to 21.1.5 and 21.2.0-rc.1. The logic normalizes URL segments by stripping leading slashes; however, it only removes a single leading slash. When an Angular SSR application is deployed behind a proxy that passes the `X-Forwarded-Prefix` header, an attacker can provide a value starting with three slashes. This vulnerability allows attackers to conduct large-scale phishing and SEO hijacking. In order to be vulnerable, the application must use Angular SSR, the application must have routes that perform internal redirects, the infrastructure (Reverse Proxy/CDN) must pass the `X-Forwarded-Prefix` header to the SSR process without sanitization, and the cache must not vary on the `X-Forwarded-Prefix` header. Versions 21.2.0-rc.1, 21.1.5, 20.3.17, and 19.2.21 contain a patch. Until the patch is applied, developers should sanitize the `X-Forwarded-Prefix` header in their`server.ts` before the Angular engine processes the request.	N/A	More Details
CVE-2026-2584	A critical SQL Injection (SQLi) vulnerability has been identified in the authentication module of the system. An unauthenticated, remote attacker (AV:N/PR:N) can exploit this flaw by sending specially crafted SQL queries through the login interface. Due to low attack complexity (AC:L) and the absence of specific requirements (AT:N), the vulnerability allows for a total compromise of the system's configuration data (VC:H/VI:H). While the availability of the service remains unaffected (VA:N), the breach may lead to a limited exposure of sensitive information regarding subsequent or interconnected systems (SC:L).	N/A	More Details
CVE-2025-10350	SQL Injection vulnerability in "imageserver" module when processing C-FIND queries in CGM NETRAAD software allows attacker connected to PACS gaining access to database, including data processed by GCM CLININET software.This issue affects CGM NETRAAD with imageserver module in versions before 7.9.0.	N/A	More Details
CVE-2026-3266	Missing Authorization vulnerability in OpenText™ Filr allows Authentication Bypass. The vulnerability could allow unauthenticated users to get XSRF token and do RPC with carefully crafted programs. This issue affects Filr: through 25.1.2.	N/A	More Details