SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 March 2026

Generated on 18 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-2026-26954	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.34, it is possible to obtain arrays containing Function, which allows escaping the sandbox. Given an array containing Function, and Object.fromEntries, it is possible to construct {[p]: Function} where p is any constructible property. This vulnerability is fixed in 0.8.34.	10.0	More Details
CVE-2026-3611	The Honeywell IQ4x building management controller, exposes its full web-based HMI without authentication in its factory-default configuration. With no user module configured, security is disabled by design and the system operates under a System Guest (level 100) context, granting read/write privileges to any party able to reach the HTTP interface. Authentication controls are only enforced after a web user is created via U.htm, which dynamically enables the user module. Because this function is accessible prior to authentication, a remote user can create a new account with administrative read/write permissions enabling the user module and imposing authentication under attacker-controlled credentials. This action can effectively lock legitimate operators out of local and web-based configuration and administration.	10.0	More Details
CVE-2026-31957	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. From 3.0.0 to before 3.1.0, if Himmelblau is deployed without a configured tenant domain in himmelblau.conf, authentication is not tenant-scoped. In this mode, Himmelblau can accept authentication attempts for arbitrary Entra ID domains by dynamically registering providers at runtime. This behavior is intended for initial/local bootstrap scenarios, but it can create risk in remote authentication environments. This vulnerability is fixed in 3.1.0.	10.0	More Details
CVE-2026-27897	Vociferous provides cross-platform, offline speech-to-text with local AI refinement. Prior to 4.4.2, the vulnerability exists in src/api/system.py within the export_file route. The application accepts a JSON payload containing a filename and content. While the developer intended for a native UI dialog to handle the file path, the API does not validate the filename string before it is processed by the backends filesystem logic. Because the API is unauthenticated and the CORS configuration in app.py is overly permissive (allow_origins=["*"] or allowing localhost), an external attacker can bypass the UI entirely. By using directory traversal sequences (../), an attacker can force the app to write arbitrary data to any location accessible by the current user's permissions. This vulnerability is fixed in 4.4.2.	10.0	More Details
CVE-2026-31852	Jellyfin is an open-source media system. The code-quality.yml GitHub Actions workflow in jellyfin/jellyfin-ios is vulnerable to arbitrary code execution via pull requests from forked repositories. Due to the workflow's elevated permissions (nearly all write permissions), this vulnerability enables full repository takeover of jellyfin/jellyfin-ios, exfiltration of highly privileged secrets, Apple App Store supply chain attack, GitHub Container Registry (ghcr.io) package poisoning, and full jellyfin organization compromise via cross-repository token usage. Note: This is not a code vulnerability, but a vulnerability in the GitHub Actions workflows. No new version is required for this GHSA and end users do not need to take any actions.	10.0	More Details
CVE-2026-32621	Apollo Federation is an architecture for declaratively composing APIs into a unified graph. Prior to 2.9.6, 2.10.5, 2.11.6, 2.12.3, and 2.13.2, a vulnerability exists in query plan execution within the gateway that may allow pollution of Object.prototype in certain scenarios. A malicious client may be able to pollute Object.prototype in gateway directly by crafting operations with field aliases and/or variable names that target prototype-inheritable properties. Alternatively, if a subgraph were to be compromised by a malicious actor, they may be able to pollute Object.prototype in gateway by crafting JSON response payloads that target prototype-inheritable properties. This vulnerability is fixed in 2.9.6, 2.10.5, 2.11.6, 2.12.3, and 2.13.2.	9.9	More Details
CVE-2026-32306	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.23, the telemetry aggregation API accepts user-controlled aggregationType, aggregateColumnName, and aggregationTimestampColumnName parameters and interpolates them directly into ClickHouse SQL queries via the .append() method (documented as "trusted SQL"). There is no allowlist, no parameterized query binding, and no input validation. An authenticated user can inject arbitrary SQL into ClickHouse, enabling full database read (including telemetry data from all tenants), data modification, and potential remote code execution via ClickHouse table functions. This vulnerability is fixed in 10.0.23.	9.9	More Details
CVE-2025-66956	Insecure Access Control in Contact Plan, E-Mail, SMS and Fax components in Asseco SEE Live 2.0 allows remote attackers to access and execute attachments via a computable URL.	9.9	More Details
	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Prior to 1.0.477, 1.1.12,		

CVE-2026-27591	and 1.2.12, Winter CMS allowed authenticated backend users to escalate their accounts level of access to the system by modifying the roles / permissions assigned to their account through specially crafted requests to the backend while logged in. To actively exploit this security issue, an attacker would need access to the Backend with a user account with any level of access. This vulnerability is fixed in 1.0.477, 1.1.12, and 1.2.12.	9.9	More Details
CVE-2026-21708	A vulnerability allowing a Backup Viewer to perform remote code execution (RCE) as the postgres user.	9.9	More Details
CVE-2026-21666	A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.	9.9	More Details
CVE-2026-21667	A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.	9.9	More Details
CVE-2026-21669	A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.	9.9	More Details
CVE-2026-32248	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.12 and 8.6.38, an unauthenticated attacker can take over any user account that was created with an authentication provider that does not validate the format of the user identifier (e.g. anonymous authentication). By sending a crafted login request, the attacker can cause the server to perform a pattern-matching query instead of an exact-match lookup, allowing the attacker to match an existing user and obtain a valid session token for that user's account. Both MongoDB and PostgreSQL database backends are affected. Any Parse Server deployment that allows anonymous authentication (enabled by default) is vulnerable. This vulnerability is fixed in 9.6.0-alpha.12 and 8.6.38.	9.8	More Details
CVE-2026-25823	HMS Networks Ewon Flexy with firmware before 15.0s4, Cosy+ with firmware 22.xx before 22.1s6, and Cosy+ with firmware 23.xx before 23.0s3 have a stack buffer overflow that leads to a Denial of Service, which can also be exploited to achieve Unauthenticated Remote Code Execution.	9.8	More Details
CVE-2016-20026	ZKTeco ZKBioSecurity 3.0 contains hardcoded credentials in the bundled Apache Tomcat server that allow unauthenticated attackers to access the manager application. Attackers can authenticate with hardcoded credentials stored in tomcat-users.xml to upload malicious WAR archives containing JSP applications and execute arbitrary code with SYSTEM privileges.	9.8	More Details
CVE-2026-26793	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the set_config function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	9.8	More Details
CVE-2025-70245	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWizardSelectMode.	9.8	More Details
CVE-2026-31806	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, the gdi_surface_bits() function processes SURFACE_BITS_COMMAND messages sent by the RDP server. When the command is handled using NSCodec, the bmp.width and bmp.height values provided by the server are not properly validated against the actual desktop dimensions. A malicious RDP server can supply crafted bmp.width and bmp.height values that exceed the expected surface size. Because these values are used during bitmap decoding and memory operations without proper bounds checking, this can lead to a heap buffer overflow. Since the attacker can also control the associated pixel data transmitted by the server, the overflow may be exploitable to overwrite adjacent heap memory. This vulnerability is fixed in 3.24.0.	9.8	More Details
CVE-2026-32304	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Prior to 3.0.14, the create_function(args, code) function passes both parameters directly to the Function constructor without any sanitization, allowing arbitrary code execution. This is distinct from CVE-2026-29091 which was call_user_func_array using eval() in v2.x. This finding affects create_function using new Function() in v3.x. This vulnerability is fixed in 3.0.14.	9.8	More Details
CVE-2026-32746	telnetd in GNU inetutils through 2.7 allows an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption handler because add_slc does not check whether the buffer is full.	9.8	More Details
CVE-2026-26792	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain multiple command injection vulnerabilities in the set_upgrade function via the modem_url, target_version, current_version, firmware_upload, hash_type, hash_value, and upgrade_type parameters. These vulnerabilities allow attackers to execute arbitrary commands via a crafted input.	9.8	More Details
CVE-2026-3891	The Pix for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check and missing file type validation in the 'lkn_pix_for_woocommerce_c6_save_settings' function in all versions up to, and including, 1.5.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2016-20024	ZKTeco ZKTime.Net 3.0.1.6 contains an insecure file permissions vulnerability that allows unprivileged users to escalate privileges by modifying executable files. Attackers can exploit world-writable permissions on the ZKTimeNet3.0 directory and its contents to replace executable files with malicious binaries for privilege escalation.	9.8	More Details
CVE-2026-23813	A vulnerability has been identified in the web-based management interface of AOS-CX switches that could potentially allow an unauthenticated remote actor to circumvent existing authentication controls. In some cases this could enable resetting the admin password.	9.8	More Details
CVE-2016-20030	ZKTeco ZKBioSecurity 3.0 contains a user enumeration vulnerability that allows unauthenticated attackers to discover valid usernames by submitting partial characters via the username parameter. Attackers can send requests to the authLoginAction!login.do script with varying username inputs to enumerate valid user accounts based on application responses.	9.8	More Details
CVE-2026-26791	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the string port parameter in the enable_echo_server function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	9.8	More Details
CVE-2026-4312	GCB/FCB Audit Software developed by DrangSoft has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly access certain APIs to create a new administrative account.	9.8	More Details
CVE-2025-69902	A command injection vulnerability in the minimal_wrapper.py component of kubectl-mcp-server v1.2.0 allows attackers to execute arbitrary commands via injecting arbitrary shell metacharacters.	9.8	More Details
CVE-2026-32267	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.6 and from version 5.0.0-RC1 to before version 5.9.12, a low-privilege user (or an unauthenticated user who has been sent a shared URL) can escalate their privileges to admin by abusing UsersController->actionImpersonateWithToken. This issue has been patched in versions 4.17.6 and 5.9.12.	9.8	More Details

CVE-2026-28430	Chamilo LMS is a learning management system. Prior to version 1.11.34, there is an unauthenticated SQL injection vulnerability which allows remote attackers to execute arbitrary SQL commands via the custom_dates parameter. By chaining this with a predictable legacy password reset mechanism, an attacker can achieve full administrative account takeover without any prior credentials. The vulnerability also exposes the entire database, including PII and system configurations. This issue has been patched in version 1.11.34.	9.8	More Details
CVE-2025-69809	A write-what-where condition in p2r3 Bareiron commit 8e4d40 allows unauthenticated attackers to write arbitrary values to memory, enabling arbitrary code execution via a crafted packet.	9.8	More Details
CVE-2026-4254	A weakness has been identified in Tenda AC8 up to 16.03.50.11. This vulnerability affects the function doSystemCmd of the file /goform/SysToolChangePwd of the component HTTP Endpoint. This manipulation of the argument local_2c causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-4252	A vulnerability was identified in Tenda AC8 16.03.50.11. Affected by this issue is the function check_is_ipv6 of the component IPv6 Handler. The manipulation leads to reliance on ip address for authentication. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2025-62319	Boolean-Based SQL Injection is a type of blind SQL injection where an attacker manipulates SQL queries by injecting Boolean conditions (TRUE or FALSE) into application input fields. Instead of returning database errors or visible data, the application responds differently depending on whether the injected condition evaluates to true or false. This allows an attacker to inject arbitrary SQL into backend configuration queries executed within the application.	9.8	More Details
CVE-2026-4184	A vulnerability was detected in D-Link DIR-816 1.10CNB05. Affected by this vulnerability is an unknown functionality of the file /goform/form2Wl5BasicSetup.cgi of the component goahead. Performing a manipulation of the argument pskValue results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2026-4183	A security vulnerability has been detected in D-Link DIR-816 1.10CNB05. Affected is an unknown function of the file /goform/form2WlanBasicSetup.cgi of the component goahead. Such manipulation of the argument pskValue leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2026-4182	A weakness has been identified in D-Link DIR-816 1.10CNB05. This impacts an unknown function of the file /goform/form2Wl5RepeaterStep2.cgi of the component goahead. This manipulation of the argument key1/key2/key3/key4/pskValue causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2026-4181	A security flaw has been discovered in D-Link DIR-816 1.10CNB05. This affects an unknown function of the file /goform/form2RepeaterStep2.cgi of the component goahead. The manipulation of the argument key1/key2/key3/key4/pskValue 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. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2026-4170	A weakness has been identified in Topsec TopACM 3.0. Affected by this vulnerability is an unknown functionality of the file /view/systemConfig/management/nmc_sync.php of the component HTTP Request Handler. Executing a manipulation of the argument template_path can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-4164	A flaw has been found in Wavlink WL-WN578W2 221110. Impacted is the function Delete_Mac_list/SetName/GuestWifi of the file /cgi-bin/wireless.cgi of the component POST Request Handler. Executing a manipulation can lead to command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. It is recommended to upgrade the affected component.	9.8	More Details
CVE-2026-4163	A vulnerability was detected in Wavlink WL-WN579A3 220323. This issue affects the function SetName/GuestWifi of the file /cgi-bin/wireless.cgi of the component POST Request Handler. Performing a manipulation results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. Upgrading the affected component is recommended.	9.8	More Details
CVE-2025-69246	Raytha CMS does not have any brute force protection mechanism implemented. It allows an attacker to send multiple automated logon requests without triggering lockout, throttling, or step-up challenges. This issue was fixed in version 1.4.6.	9.8	More Details
CVE-2017-20224	Telesquare SKT LTE Router SDT-CS3B1 version 1.2.0 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious content by exploiting enabled WebDAV HTTP methods. Attackers can use PUT, DELETE, MKCOL, MOVE, COPY, and PROPPATCH methods to upload executable code, delete files, or manipulate server content for remote code execution or denial of service.	9.8	More Details
CVE-2017-20223	Telesquare SKT LTE Router SDT-CS3B1 firmware version 1.2.0 contains an insecure direct object reference vulnerability that allows attackers to bypass authorization and access resources by manipulating user-supplied input parameters. Attackers can directly reference objects in the system to retrieve sensitive information and access functionalities without proper access controls.	9.8	More Details
CVE-2026-26795	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the module parameter in the M.get_system_log function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	9.8	More Details
CVE-2026-21994	Vulnerability in the Oracle Edge Cloud Infrastructure Designer and Visualisation Toolkit product of Oracle Open Source Projects (component: Desktop). The supported version that is affected is 0.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Edge Cloud Infrastructure Designer and Visualisation Toolkit. Successful attacks of this vulnerability can result in takeover of Oracle Edge Cloud Infrastructure Designer and Visualisation Toolkit. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-31856	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. A SQL injection vulnerability exists in the PostgreSQL storage adapter when processing Increment operations on nested object fields using dot notation (e.g., stats.counter). The amount value is interpolated directly into the SQL query without parameterization or type validation. An attacker who can send write requests to the Parse Server REST API can inject arbitrary SQL subqueries to read any data from the database, bypassing CLPs and ACLs. MongoDB deployments are not affected. This vulnerability is fixed in	9.8	More Details

	9.6.0-alpha.3 and 8.6.29.		
CVE-2018-25159	Epross AVCON6 systems management platform contains an object-graph navigation language (OGNL) injection vulnerability that allows unauthenticated attackers to execute arbitrary commands by injecting malicious OGNL expressions. Attackers can send crafted requests to the login.action endpoint with OGNL payloads in the redirect parameter to instantiate ProcessBuilder objects and execute system commands with root privileges.	9.8	More Details
CVE-2026-31840	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.2 and 8.6.28, an attacker can use a dot-notation field name in combination with the sort query parameter to inject SQL into the PostgreSQL database through an improper escaping of sub-field values in dot-notation queries. The vulnerability may also affect queries that use dot-notation field names with the distinct and where query parameters. This vulnerability only affects deployments using a PostgreSQL database. This vulnerability is fixed in 9.6.0-alpha.2 and 8.6.28.	9.8	More Details
CVE-2019-25468	NetGain EM Plus 10.1.68 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious parameters to the script_test.jsp endpoint. Attackers can send POST requests with shell commands embedded in the 'content' parameter to execute code and retrieve command output.	9.8	More Details
CVE-2019-25471	FileThingie 2.5.7 contains an arbitrary file upload vulnerability that allows attackers to upload malicious files by sending ZIP archives through the ft2.php endpoint. Attackers can upload ZIP files containing PHP shells, use the unzip functionality to extract them into accessible directories, and execute arbitrary commands through the extracted PHP files.	9.8	More Details
CVE-2019-25487	SAPIDO RB-1732 V2.0.43 contains a remote command execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the formSysCmd endpoint. Attackers can send POST requests with the sysCmd parameter containing shell commands to execute code on the device with router privileges.	9.8	More Details
CVE-2026-31874	Taskosaur is an open source project management platform with conversational AI for task execution in-app. In 1.0.0, the application does not properly validate or restrict the role parameter during the user registration process. An attacker can manually modify the request payload and assign themselves elevated privileges. Because the backend does not enforce role assignment restrictions or ignore client-supplied role parameters, the server accepts the manipulated value and creates the account with SUPER_ADMIN privileges. This allows any unauthenticated attacker to register a fully privileged administrative account.	9.8	More Details
CVE-2026-31877	Frappe is a full-stack web application framework. Prior to 15.84.0 and 14.99.0, a specially crafted request made to a certain endpoint could result in SQL injection, allowing an attacker to extract information they wouldn't otherwise be able to. This vulnerability is fixed in 15.84.0 and 14.99.0.	9.8	More Details
CVE-2025-70082	An issue in Lantronix EDS3000PS v.3.1.0.0R2 allows an attacker to execute arbitrary code and obtain sensitive information via the ltrx_evo component	9.8	More Details
CVE-2026-31896	WeGIA is a web manager for charitable institutions. Prior to version 3.6.6, a critical SQL injection vulnerability exists in the WeGIA application. The remover_produto_ocultar.php script uses extract($_REQUEST) to populate local variables and then directly concatenates these variables into a SQL query executed via PDO::query. This allows an authenticated (or auth-bypassed) attacker to execute arbitrary SQL commands. This can be used to exfiltrate sensitive data from the database or, as demonstrated in this PoC, cause a time-based delay (denial of service). This vulnerability is fixed in 3.6.6.	9.8	More Details
CVE-2026-31900	Black is the uncompromising Python code formatter. Black provides a GitHub action for formatting code. This action supports an option, use_pyproject: true, for reading the version of Black to use from the repository pyproject.toml. A malicious pull request could edit pyproject.toml to use a direct URL reference to a malicious repository. This could lead to arbitrary code execution in the context of the GitHub Action. Attackers could then gain access to secrets or permissions available in the context of the action. Version 26.3.0 fixes this vulnerability.	9.8	More Details
CVE-2026-31976	xygeni-action is the GitHub Action for Xygeni Scanner. On March 3, 2026, an attacker with access to compromised credentials created a series of pull requests (#46, #47, #48) injecting obfuscated shell code into action.yml. The PRs were blocked by branch protection rules and never merged into the main branch. However, the attacker used the compromised GitHub App credentials to move the mutable v5 tag to point at the malicious commit (4bf1d4e19ad81a3e8d4063755ae0f482dd3baf12) from one of the unmerged PRs. This commit remained in the repository's git object store, and any workflow referencing @v5 would fetch and execute it. This is a supply chain compromise via tag poisoning. Any GitHub Actions workflow referencing xygeni/xygeni-action@v5 during the affected window (approximately March 3–10, 2026) executed a C2 implant that granted the attacker arbitrary command execution on the CI runner for up to 180 seconds per workflow run.	9.8	More Details
CVE-2025-67041	An issue was discovered in Lantronix EDS3000PS 3.1.0.0R2. The host parameter of the TFTP client in the Filesystem Browser page is not properly sanitized. This can be exploited to escape from the original command and execute an arbitrary one with root privileges.	9.8	More Details
CVE-2025-67038	An issue was discovered in Lantronix EDS5000 2.1.0.0R3. The HTTP RPC module executes a shell command to write logs when user's authantication fails. The username is directly concatenated with the command without any sanitization. This allow attackers to inject arbitrary OS commands into the username parameter. Injected commands are executed with root privileges.	9.8	More Details
CVE-2025-70024	An issue pertaining to CWE-89: Improper Neutralization of Special Elements used in an SQL Command was discovered in benkeen generatedata 4.0.14.	9.8	More Details
CVE-2025-67035	An issue was discovered in Lantronix EDS5000 2.1.0.0R3. The SSH Client and SSH Server pages are affected by multiple OS injection vulnerabilities due to missing sanitization of input parameters. An attacker can inject arbitrary commands in delete actions of various objects, such as server keys, users, and known hosts. Commands are executed with root privileges.	9.8	More Details
CVE-2026-30741	A remote code execution (RCE) vulnerability in OpenClaw Agent Platform v2026.2.6 allows attackers to execute arbitrary code via a Request-Side prompt injection attack.	9.8	More Details
CVE-2025-70041	An issue pertaining to CWE-259: Use of Hard-coded Password was discovered in oslabs-beta ThermaKube master.	9.8	More Details
CVE-2026-28229	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Prior to 4.0.2 and 3.7.11, Workflow templates endpoints allow any client to retrieve WorkflowTemplates (and ClusterWorkflowTemplates). Any request with a Authorization: Bearer nothing token can leak sensitive template content, including embedded Secret manifests. This vulnerability is fixed in 4.0.2 and 3.7.11.	9.8	More Details
CVE-2026-	AdGuard Home is a network-wide software for blocking ads and tracking. Prior to 0.107.73, an unauthenticated remote attacker can bypass all authentication in AdGuardHome by sending an HTTP/1.1 request that requests an upgrade to HTTP/2 cleartext		

32136	(h2c). Once the upgrade is accepted, the resulting HTTP/2 connection is handled by the inner mux, which has no authentication middleware attached. All subsequent HTTP/2 requests on that connection are processed as fully authenticated, regardless of whether any credentials were provided. This vulnerability is fixed in 0.107.73.	9.8	More Details
CVE-2026-3826	IFTOP developed by WellChoose has a Local File Inclusion vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server.	9.8	More Details
CVE-2025-59388	A use of hard-coded password vulnerability has been reported to affect Hyper Data Protector. The remote attackers can then exploit the vulnerability to gain unauthorized access. We have already fixed the vulnerability in the following version: Hyper Data Protector 2.3.1.455 and later	9.8	More Details
CVE-2026-3059	SGLang's multimodal generation module is vulnerable to unauthenticated remote code execution through the ZMQ broker, which deserializes untrusted data using pickle.loads() without authentication.	9.8	More Details
CVE-2026-3060	SGLang' encoder parallel disaggregation system is vulnerable to unauthenticated remote code execution through the disaggregation module, which deserializes untrusted data using pickle.loads() without authentication.	9.8	More Details
CVE-2026-2631	The Datalogics Ecommerce Delivery WordPress plugin before 2.6.60 exposes an unauthenticated REST endpoint that allows any remote user to modify the option `datalogics_token` without verification. This token is subsequently used for authentication in a protected endpoint that allows users to perform arbitrary WordPress `update_option()` operations. Attackers can use this to enable registartion and to set the default role as Administrator.	9.8	More Details
CVE-2026-31871	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.5 and 8.6.31, a SQL injection vulnerability exists in the PostgreSQL storage adapter when processing Increment operations on nested object fields using dot notation (e.g., stats.counter). The sub-key name is interpolated directly into SQL string literals without escaping. An attacker who can send write requests to the Parse Server REST API can inject arbitrary SQL via a crafted sub-key name containing single quotes, potentially executing commands or reading data from the database, bypassing CLPs and ACLs. Only Postgres deployments are affected. This vulnerability is fixed in 9.6.0-alpha.5 and 8.6.31.	9.8	More Details
CVE-2026-30903	External Control of File Name or Path in the Mail feature of Zoom Workplace for Windows before 6.6.0 may allow an unauthenticated user to conduct an escalation of privilege via network access.	9.6	More Details
CVE-2026-28792	Tina is a headless content management system. Prior to 2.1.8 , the TinaCMS CLI dev server combines a permissive CORS configuration (Access-Control-Allow-Origin: *) with the path traversal vulnerability (previously reported) to enable a browser-based drive-by attack. A remote attacker can enumerate the filesystem, write arbitrary files, and delete arbitrary files on developer's machines by simply tricking them into visiting a malicious website while tinacms dev is running. This vulnerability is fixed in 2.1.8.	9.6	More Details
CVE-2026-32626	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, AnythingLLM Desktop contains a Streaming Phase XSS vulnerability in the chat rendering pipeline that escalates to Remote Code Execution on the host OS due to insecure Electron configuration. This works with default settings and requires no user interaction beyond normal chat usage. The custom markdown-it image renderer in frontend/src/utils/chat/markdown.js interpolates token.content directly into the alt attribute without HTML entity escaping. The PromptReply component renders this output via dangerouslySetInnerHTML without DOMPurify sanitization — unlike HistoricalMessage which correctly applies DOMPurify.sanitize().	9.6	More Details
CVE-2026-3916	Out of bounds read in Web Speech in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-32096	Plunk is an open-source email platform built on top of AWS SES. Prior to 0.7.0, a Server-Side Request Forgery (SSRF) vulnerability existed in the SNS webhook handler. An unauthenticated attacker could send a crafted request that caused the server to make an arbitrary outbound HTTP GET request to any host accessible from the server. This vulnerability is fixed in 0.7.0.	9.3	More Details
CVE-2026-32301	Centrifugo is an open-source scalable real-time messaging server. Prior to 6.7.0, Centrifugo is vulnerable to Server-Side Request Forgery (SSRF) when configured with a dynamic JWKS endpoint URL using template variables (e.g. {{tenant}}). An unauthenticated attacker can craft a JWT with a malicious iss or aud claim value that gets interpolated into the JWKS fetch URL before the token signature is verified, causing Centrifugo to make an outbound HTTP request to an attacker-controlled destination. This vulnerability is fixed in 6.7.0.	9.3	More Details
CVE-2026-21671	A vulnerability allowing an authenticated user with the Backup Administrator role to perform remote code execution (RCE) in high availability (HA) deployments of Veeam Backup & Replication.	9.1	More Details
CVE-2026-32298	The Angeet ES3 KVM does not properly sanitize user-supplied variables parsed by the 'cfg.lua' script, allowing an authenticated attacker to execute OS-level commands.	9.1	More Details
CVE-2026-25770	Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 3.9.0 and prior to version 4.14.3, a privilege escalation vulnerability exists in the Wazuh Manager's cluster synchronization protocol. The `wazuh-clusterd` service allows authenticated nodes to write arbitrary files to the manager's file system with the permissions of the `wazuh` system user. Due to insecure default permissions, the `wazuh` user has write access to the manager's main configuration file (`/var/ossec/etc/ossec.conf`). By leveraging the cluster protocol to overwrite `ossec.conf`, an attacker can inject a malicious `<localfile>` command block. The `wazuh-logcollector` service, which runs as root, parses this configuration and executes the injected command. This chain allows an attacker with cluster credentials to gain full Root Remote Code Execution, violating the principle of least privilege and bypassing the intended security model. Version 4.14.3 fixes the issue.	9.1	More Details
CVE-2026-25769	Wazuh is a free and open source platform used for threat prevention, detection, and response. Versions 4.0.0 through 4.14.2 have a Remote Code Execution (RCE) vulnerability due to Deserialization of Untrusted Data). All Wazuh deployments using cluster mode (master/worker architecture) and any organization with a compromised worker node (e.g., through initial access, insider threat, or supply chain attack) are impacted. An attacker who gains access to a worker node (through any means) can achieve full RCE on the master node with root privileges. Version 4.14.3 fixes the issue.	9.1	More Details
CVE-2026-25534	### Impact Spinnaker updated URL Validation logic on user input to provide sanitation on user inputted URLs for clouddriver. However, they missed that Java URL objects do not correctly handle underscores on parsing. This led to a bypass of the previous CVE (CVE-2025-61916) through the use of carefully crafted URLs. Note, Spinnaker found this not just in that CVE, but in the existing URL validations in Orca fromUrl expression handling. This CVE impacts BOTH artifacts as a result. ### Patches This has been merged and will be available in versions 2025.4.1, 2025.3.1, 2025.2.4 and 2026.0.0. ### Workarounds You can disable the various artifacts on this system to work around these limits.	9.1	More Details

CVE-2026-4177	YAML::Syck versions through 1.36 for Perl has several potential security vulnerabilities including a high-severity heap buffer overflow in the YAML emitter. The heap overflow occurs when class names exceed the initial 512-byte allocation. The base64 decoder could read past the buffer end on trailing newlines. strtok mutated n->type_id in place, corrupting shared node data. A memory leak occurred in syck_hdlr_add_anchor when a node already had an anchor. The incoming anchor string 'a' was leaked on early return.	9.1	More Details
CVE-2026-25818	HMS Networks Ewon Flexy with firmware before 15.0s4, Cosy+ with firmware 22.xx before 22.1s6, and Cosy+ with firmware 23.xx before 23.0s3 have weak entropy for authentication cookies, allowing an attacker with a stolen session cookie to find the user password by brute-forcing an encryption parameter.	9.1	More Details
CVE-2026-31862	Cloud CLI (aka Claude Code UI) is a desktop and mobile UI for Claude Code, Cursor CLI, Codex, and Gemini-CLI. Prior to 1.24.0, multiple Git-related API endpoints use execAsync() with string interpolation of user-controlled parameters (file, branch, message, commit), allowing authenticated attackers to execute arbitrary OS commands. This vulnerability is fixed in 1.24.0.	9.1	More Details
CVE-2026-31886	Dagu is a workflow engine with a built-in Web user interface. Prior to 2.2.4, the dagRunId request field accepted by the inline DAG execution endpoints is passed directly into filepath.Join to construct a temporary directory path without any format validation. Go's filepath.Join resolves .. segments lexically, so a caller can supply a value such as ".." to redirect the computed directory outside the intended /tmp/<name>/<id> path. A deferred cleanup function that calls os.RemoveAll on that directory then runs unconditionally when the HTTP handler returns, deleting whatever directory the traversal resolved to. With dagRunId set to "..", the resolved directory is the system temporary directory (/tmp on Linux). On non-root deployments, os.RemoveAll("/tmp") removes all files in /tmp owned by the dagu process user, disrupting every concurrent dagu run that has live temp files. On root or Docker deployments, the call removes the entire contents of /tmp, causing a system-wide denial of service. This vulnerability is fixed in 2.2.4.	9.1	More Details
CVE-2025-69808	An out-of-bounds memory access (OOB) in p2r3 Bareiron commit 8e4d40 allows unauthenticated attackers to access sensitive information and cause a Denial of Service (DoS) via supplying a crafted packet.	9.1	More Details
CVE-2026-27962	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.9, a JWK Header Injection vulnerability in authlib's JWS implementation allows an unauthenticated attacker to forge arbitrary JWT tokens that pass signature verification. When key=None is passed to any JWS deserialization function, the library extracts and uses the cryptographic key embedded in the attacker-controlled JWT jwk header field. An attacker can sign a token with their own private key, embed the matching public key in the header, and have the server accept the forged token as cryptographically valid — bypassing authentication and authorization entirely. This issue has been patched in version 1.6.9.	9.1	More Details
CVE-2026-23489	Fields is a GLPI plugin that allows users to add custom fields on GLPI items forms. Prior to version 1.23.3, it is possible to execute arbitrary PHP code from users that are allowed to create dropdowns. This issue has been patched in version 1.23.3.	9.1	More Details
CVE-2025-67039	An issue was discovered in Lantronix EDS3000PS 3.1.0.0R2. The authentication on management pages can be bypassed by appending a specific suffix to the URL and by sending an Authorization header that uses "admin" as the username.	9.1	More Details
CVE-2026-32367	Improper Control of Generation of Code ('Code Injection') vulnerability in Yannick Lefebvre Modal Dialog modal-dialog allows Remote Code Inclusion.This issue affects Modal Dialog: from n/a through <= 3.5.16.	9.1	More Details
CVE-2026-27478	Unity Catalog is an open, multi-modal Catalog for data and AI. In 0.4.0 and earlier, a critical authentication bypass vulnerability exists in the Unity Catalog token exchange endpoint (/api/1.0/unity-control/auth/tokens). The endpoint extracts the issuer (iss) claim from incoming JWTs and uses it to dynamically fetch the JWKS endpoint for signature validation without validating that the issuer is a trusted identity provider.	9.1	More Details
CVE-2026-32133	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Prior to 6.1.0, a blind SSRF vulnerability exists in 2FAuth that allows authenticated users to make arbitrary HTTP requests from the server to internal networks and cloud metadata endpoints. The image parameter in OTP URL is not properly validated for internal / private IP addresses before making HTTP requests. While the previous fix added response validation to ensure only valid images are stored but HTTP request is still made to arbitrary URLs before this validation occurs. This vulnerability is fixed in 6.1.0.	9.1	More Details
CVE-2023-27573	netbox-docker before 2.5.0 has a superuser account with default credentials (admin password for the admin account, and 0123456789abcdef0123456789abcdef01234567 value for SUPERUSER_API_TOKEN). In practice on the public Internet, almost all users changed the password but only about 90% changed the token. Having a default token value was intentional and was valuable for the main intended use case of the netbox-docker product (isolated development networks). Some users engaged in an effort to repurpose netbox-docker for production. The documentation for this effort stated that the defaults must not be used. However, installation did not ensure non-default values. The Supplier was aware of the CVE ID assignment and did not object to the assignment.	9.0	More Details
CVE-2026-3564	A condition in ScreenConnect may allow an actor with access to server-level cryptographic material used for authentication to obtain unauthorized access, including elevated privileges, in certain scenarios.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	
CVE-2026-31889	Shopware is an open commerce platform. Prior to 6.6.10.15 and 6.7.8.1, a vulnerability in the Shopware app registration flow that could, under specific conditions, attacker possessed the relevant app-side secret. By abusing app re-registration, an attacker could redirect app traffic to an attacker-controlled domain and potenti
CVE-2026-31979	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. Prior to 3.1.0 and 2.3.8, the himmelblaud-tasks daemon, running as root, writes Ker
CVE-2026-4227	A security vulnerability has been detected in LB-LINK BL-WR9000 2.4.9. The impacted element is the function sub_44D844 of the file /goform/get_hidessid_cfg. The
CVE-2026-28519	arduino-TuyaOpen before version 1.2.1 contains a heap-based buffer overflow vulnerability in the DnsServer component. An attacker on the same local area netwo
CVE-	

2026-4211	A weakness has been identified in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DN attacks.
CVE-2026-26794	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a SQL injection vulnerability via the add_group() function. This vulnerability allows attackers to execute ar
CVE-2026-4212	A security vulnerability has been detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DN
CVE-2026-4213	A vulnerability was detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-3
CVE-2026-1993	The ExactMetrics – Google Analytics Dashboard for WordPress plugin is vulnerable to Improper Privilege Management in versions 7.1.0 through 9.0.2. This is due to user, not enable that user to delegate access to everyone. By setting `save_settings` to include `subscriber`, an attacker can grant plugin administrative access to
CVE-2026-1992	The ExactMetrics – Google Analytics Dashboard for WordPress plugin is vulnerable to Insecure Direct Object Reference in versions 8.6.0 through 9.0.2. This is due t allowing them to install arbitrary plugins and achieve Remote Code Execution. This vulnerability only affects sites on which administrator has given other user type
CVE-2026-4214	A flaw has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, D
CVE-2026-31861	Cloud CLI (aka Claude Code UI) is a desktop and mobile UI for Claude Code, Cursor CLI, Codex, and Gemini-CLI. Prior to 1.24.0, The /api/user/git-config endpoint cor configuration endpoint. This vulnerability is fixed in 1.24.0.
CVE-2026-21668	A vulnerability allowing an authenticated domain user to bypass restrictions and manipulate arbitrary files on a Backup Repository.
CVE-2026-4226	A weakness has been identified in LB-LINK BL-WR9000 2.4.9. The affected element is the function sub_44E8D0 of the file /goform/get_virtual_cfg. Executing a mani
CVE-2026-31844	An authenticated SQL Injection vulnerability (CWE-89) exists in the Koha staff interface in the /cgi-bin/koha/suggestion/suggestion.pl endpoint due to improper vali
CVE-2026-3936	Use after free in WebView in Google Chrome on Android prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML
CVE-2026-32355	Deserialization of Untrusted Data vulnerability in Crocoblock JetEngine jet-engine allows Object Injection.This issue affects JetEngine: from n/a through < 3.8.4.1.
CVE-2026-20046	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated, local attacker to elevate privileges and without authorization checks.
CVE-2023-43010	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.2 and iPadOS 17.2, macOS Sonoma 14.2, Safari 17.2, iOS 16.7.15 and iPadO
CVE-2025-69240	Raytha CMS allows an attacker to spoof `X-Forwarded-Host` or `Host` headers to attacker controlled domain. The attacker (who knows the victim's email address)
CVE-2026-3970	A flaw has been found in Tenda i3 1.0.0.6(2204). Affected is the function formwrlSSIDget of the file /goform/wifiSSIDget. Executing a manipulation of the argument
CVE-2025-54920	This issue affects Apache Spark: before 3.5.7 and 4.0.1. Users are recommended to upgrade to version 3.5.7 or 4.0.1 and above, which fixes the issue. Summary A vulnerability arises because the Spark History Server uses Jackson polymorphic deserialization with @JsonTypeInfo.Id.CLASS on SparkListenerEvent objects, allowin event logs. For example, the attacker can force the History Server to open a JDBC connection to a remote attacker-controlled server, demonstrating remote comma 4. The Spark History Server initiates a JDBC connection to the attacker’s server, confirming the injection. Impact An attacker with write access to Spark event logs c
CVE-2026-3971	A vulnerability has been found in Tenda i3 1.0.0.6(2204). Affected by this vulnerability is the function formwrlSSIDset of the file /goform/wifiSSIDset. The manipulat
CVE-2025-15540	"Functions" module in Raytha CMS allows privileged users to write custom code to add functionality to application. Due to a lack of sandboxing or access restriction
CVE-2025-13067	The Royal Addons for Elementor plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 1.7.1049. This is due to insufficient fi
CVE-2025-69784	A local, non-privileged attacker can abuse a vulnerable IOCTL interface exposed by the OpenEDR 2.5.1.0 kernel driver to modify the DLL injection path used by the

CVE-2026-3972	A vulnerability was found in Tenda W3 1.0.0.3(2204). Affected by this issue is the function formSetCfm of the file /goform/setcfm of the component HTTP Handler. T
CVE-2026-31858	Craft is a content management system (CMS). The ElementSearchController::actionSearch() endpoint is missing the unset() protection that was added to ElementIr injection. Users should update to the patched 5.9.9 release to mitigate the issue.
CVE-2026-32059	OpenClaw version 2026.2.22-2 prior to 2026.2.23 tools.exec.safeBins validation for sort command fails to properly validate GNU long-option abbreviations, allowing
CVE-2026-23814	A vulnerability in the command parameters of a certain AOS-CX CLI command could allow a low-privilege authenticated remote attacker to inject malicious comma
CVE-2026-32060	OpenClaw versions prior to 2026.2.14 contain a path traversal vulnerability in apply_patch that allows attackers to write or delete files outside the configured work
CVE-2026-32628	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, a SQL injection vu
CVE-2025-68623	In Microsoft DirectX End-User Runtime Web Installer 9.29.1974.0, a low-privilege user can replace an executable file during the installation process, which may resu executable. When the installer executes this replaced file, it runs the attacker's code with HIGH integrity. Since code running at HIGH integrity can escalate to SYST
CVE-2025-67037	An issue was discovered in Lantronix EDS5000 2.1.0.0R3. An authenticated attacker can inject OS commands into the "tunnel" parameter when killing a tunnel con
CVE-2025-67036	An issue was discovered in Lantronix EDS5000 2.1.0.0R3. The Log Info page allows users to see log files by specifying their names. Due to a missing sanitization in
CVE-2025-67034	An issue was discovered in Lantronix EDS5000 2.1.0.0R3. An authenticated attacker can inject OS commands into the "name" parameter when deleting SSL creden
CVE-2026-32127	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, OpenEMR contains a SQL injection vul
CVE-2026-3913	Heap buffer overflow in WebML in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2026-21672	A vulnerability allowing local privilege escalation on Windows-based Veeam Backup & Replication servers.
CVE-2026-4167	A vulnerability was determined in Belkin F9K1122 1.00.33. This affects the function formReboot of the file /goform/formReboot. This manipulation of the argument
CVE-2026-3914	Integer overflow in WebML in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chr
CVE-2026-3915	Heap buffer overflow in WebML in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML p
CVE-2026-3917	Use after free in Agents in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chrom
CVE-2026-3918	Use after free in WebMCP in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chro
CVE-2026-3919	Use after free in Extensions in Google Chrome prior to 146.0.7680.71 allowed an attacker who convinced a user to install a malicious extension to potentially explo
CVE-2026-4188	A security flaw has been discovered in D-Link DIR-619L 2.06B01. The affected element is the function formSchedule of the file /goform/formSchedule of the compor
CVE-2026-3920	Out of bounds memory access in WebML in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HT
CVE-2026-3921	Use after free in TextEncoding in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (
CVE-	

2026-3922	Use after free in MediaStream in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (
CVE-2026-3923	Use after free in WebMIDI in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chro
CVE-2026-3926	Out of bounds read in V8 in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (C
CVE-2026-4043	A security vulnerability has been detected in Tenda i12 1.0.0.6(2204). The impacted element is the function formwrlSSIDget of the file /goform/wifiSSIDget. Such m
CVE-2026-3931	Heap buffer overflow in Skia in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page
CVE-2026-31857	Craft is a content management system (CMS). Prior to 5.9.9 and 4.17.4, a Remote Code Execution vulnerability exists in the Craft CMS 5 conditions system. The Ba privileges, no special permissions beyond basic control panel access, and bypasses all production hardening settings (allowAdminChanges: false, devMode: false, e
CVE-2026-3973	A vulnerability was determined in Tenda W3 1.0.0.3(2204). This affects the function formSetAutoPing of the file /goform/setAutoPing of the component POST Param
CVE-2026-20040	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating
CVE-2026-4318	A vulnerability was determined in UTT HiPER 810G up to 1.7.7-171114. Affected is the function strcpy of the file /goform/formApLbConfig. This manipulation of the
CVE-2026-3978	A vulnerability was detected in D-Link DIR-513 1.10. The impacted element is an unknown function of the file /goform/formEasySetupWizard3. The manipulation of
CVE-2026-4148	A use-after-free vulnerability can be triggered in sharded clusters by an authenticated user with the read role who issues a specially crafted $lookup or $graphLook
CVE-2026-25817	HMS Networks Ewon Flexy with firmware before 15.0s4, Cosy+ with firmware 22.xx before 22.1s6, and Cosy+ with firmware 23.xx before 23.0s3 have improper ne
CVE-2026-4042	A weakness has been identified in Tenda i12 1.0.0.6(2204). The affected element is the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet. This ma
CVE-2026-32137	Dataease is an open source data visualization analysis tool. Prior to 2.10.20, The table parameter for /de2api/datasource/previewData is directly concatenated into
CVE-2026-4008	A flaw has been found in Tenda W3 1.0.0.3(2204). This issue affects some unknown processing of the file /goform/wifiSSIDset of the component POST Parameter H
CVE-2016-20025	ZKTeco ZKAccess Professional 3.5.3 contains an insecure file permissions vulnerability that allows authenticated users to escalate privileges by modifying executab
CVE-2026-4007	A vulnerability was detected in Tenda W3 1.0.0.3(2204). This vulnerability affects unknown code of the file /goform/wifiSSIDget of the component POST Parameter
CVE-2026-4041	A security flaw has been discovered in Tenda i12 1.0.0.6(2204). Impacted is the function vos_strcpy of the file /goform/exeCommand. The manipulation of the argu
CVE-2026-32140	Dataease is an open source data visualization analysis tool. Prior to 2.10.20, By controlling the IniFile parameter, an attacker can force the JDBC driver to load an a explicitly specify the configuration file via URL parameters, which allows arbitrary files on the server to be loaded as JDBC configuration files. Within the Redshift JD
CVE-2016-20034	Wowza Streaming Engine 4.5.0 contains a privilege escalation vulnerability that allows authenticated read-only users to elevate privileges to administrator by man
CVE-2026-31895	WeGIA is a web manager for charitable institutions. Prior to version 3.6.6, WeGIA (Web gerenciador para instituições assistenciais) contains a SQL injection vulnera
CVE-2026-30881	Chamilo LMS is a learning management system. Version 1.11.34 and prior contains a SQL Injection vulnerability in the statistics AJAX endpoint. The parameters dat the database query, enabling blind time-based and conditional data extraction. This issue has been patched in version 1.11.36.
CVE-	

2026-30875	Chamilo LMS is a learning management system. Prior to version 1.11.36, an arbitrary file upload vulnerability in the H5P Import feature allows authenticated users
CVE-2025-50881	The `flow/admin/moniteur.php` script in Use It Flow administration website before 10.0.0 is vulnerable to Remote Code Execution. When handling GET requests, th Successful exploitation allows an unauthenticated or trivially authenticated attacker to execute arbitrary PHP code on the server with the privileges of the web serv
CVE-2026-3975	A security flaw has been discovered in Tenda W3 1.0.0.3(2204). This issue affects the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet of the com
CVE-2026-32097	PingPong is a platform for using large language models (LLMs) for teaching and learning. Prior to 7.27.2, an authenticated user may be able to retrieve or delete fil
CVE-2026-3909	Out of bounds write in Skia in Google Chrome prior to 146.0.7680.75 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2026-3910	Inappropriate implementation in V8 in Google Chrome prior to 146.0.7680.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted H
CVE-2026-3974	A vulnerability was identified in Tenda W3 1.0.0.3(2204). This vulnerability affects the function formexeCommand of the file /goform/exeCommand of the compone
CVE-2026-3976	A weakness has been identified in Tenda W3 1.0.0.3(2204). Impacted is the function formWifiMacFilterSet of the file /goform/WifiMacFilterSet of the component PO
CVE-2026-1090	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.6 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-21290	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab victim must browse to the page containing the vulnerable field.
CVE-2026-32627	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.37.2, when a cpp-httplib client is configured with a proxy and set_follow including any credentials or session tokens in flight. This vulnerability is fixed in 0.37.2.
CVE-2026-32366	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in robfelty Collapsing Categories collapsing-categories allows B
CVE-2026-32433	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in codepeople CP Contact Form with Paypal cp-contact-form-wi
CVE-2026-32368	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in delphiknight Geo to Lat geo-to-lat allows Blind SQL Injection.
CVE-2026-32246	Tinyauth is an authentication and authorization server. Prior to 5.0.3, the OIDC authorization endpoint allows users with a TOTP-pending session (password verified
CVE-2026-32459	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in flycart UpsellWP checkout-upsell-and-order-bumps allows Bli
CVE-2026-32422	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in levelfourdevelopment WP EasyCart wp-easycart allows Blind
CVE-2026-32365	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in robfelty Collapsing Archives collapsing-archives allows Blind
CVE-2026-31917	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP ERP erp allows SQL Injection.This issue affects W
CVE-2026-32399	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media LIbrary Assistant media-library-assistan
CVE-2026-31922	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ays Pro Fox LMS fox-lms allows Blind SQL Injection.This issue
CVE-2026-28520	arduino-TuyaOpen before version 1.2.1 contains a single-byte buffer overflow vulnerability in the WiFiMulti component. When the victim's smart hardware connects
CVE-2019-	Easy File Sharing Web Server 7.2 contains a local structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code b

25466	
CVE-2026-28793	Tina is a headless content management system. Prior to 2.1.8, the TinaCMS CLI development server exposes media endpoints that are vulnerable to path traversal configured media directory. This vulnerability is fixed in 2.1.8.
CVE-2019-25483	Comtrend AR-5310 GE31-412SSG-C01_R10.A2pG039u.d24k contains a restricted shell escape vulnerability that allows local users to bypass command restrictions
CVE-2019-25467	Verypdf docPrint Pro 8.0 contains a structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying ar
CVE-2026-4064	Missing authorization checks on multiple gRPC service endpoints in PowerShell Universal before 2026.1.4 allows an authenticated user with any valid token to bypa
CVE-2026-32110	SiYuan is a personal knowledge management system. Prior to 3.6.0, the /api/network/forwardProxy endpoint allows authenticated users to make arbitrary HTTP rec
CVE-2026-0708	A flaw was found in libucl. A remote attacker could exploit this by providing a specially crafted Universal Configuration Language (UCL) input that contains a key wi
CVE-2025-13779	Missing authentication for critical function vulnerability in ABB AWIN GW100 rev.2, ABB AWIN GW120.This issue affects AWIN GW100 rev.2: 2.0-0, 2.0-1; AWIN GW1
CVE-2025-13777	Authentication bypass by capture-replay vulnerability in ABB AWIN GW100 rev.2, ABB AWIN GW120.This issue affects AWIN GW100 rev.2: 2.0-0, 2.0-1; AWIN GW12
CVE-2019-25521	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the g
CVE-2026-32296	Sipeed NanoKVM before 2.3.1 exposes a Wi-Fi configuration endpoint without proper security checks, allowing an unauthenticated attacker with network access to
CVE-2019-25534	Netartmedia PHP Car Dealer contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious c
CVE-2019-25522	XooGallery Latest contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries by injecting SQL code throug
CVE-2026-32138	NEXULEAN is a cybersecurity portfolio & service platform for an Ethical Hacker, AI Enthusiast, and Penetration Tester. Prior to 2.0.0, a security vulnerability was ide
CVE-2019-25535	Netartmedia PHP Dating Site contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code thr
CVE-2019-25536	Netartmedia PHP Real Estate Agency 4.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting
CVE-2019-25539	202CMS v10 beta contains a blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through
CVE-2019-25540	Netartmedia PHP Mall 4.1 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries by injecting SQL code
CVE-2019-25541	Netartmedia PHP Mall 4.1 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries through unvalidated
CVE-2019-25520	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an authentication bypass vulnerability in the administration panel that allows unauthenticated attackers to gain a
CVE-2019-25537	Netartmedia Event Portal 2.0 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injec
CVE-2026-31839	Striae is a firearms examiner's comparison companion. A high-severity integrity bypass vulnerability existed in Striae's digital confirmation workflow prior to v3.0.0
CVE-2026-	xml-security is a library that implements XML signatures and encryption. Prior to versions 2.3.1 and 1.13.9, XML nodes encrypted with either aes-128-gcm, aes-192

32600	
CVE-2026-32616	Pigeon is a message board/notepad/social system/blog. Prior to 1.0.201, the application uses $_SERVER['HTTP_HOST'] without validation to construct email verifica
CVE-2026-32313	xmlseclibs is a library written in PHP for working with XML Encryption and Signatures. Prior to 3.1.5, XML nodes encrypted with either aes-128-gcm, aes-192-gcm, c
CVE-2019-25508	Jettweb Php Hazir Ilan Sitesi Scripti V2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQ
CVE-2019-25542	Netartmedia Real Estate Portal 5.0 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL co
CVE-2019-25538	202CMS v10 beta contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the l
CVE-2019-25526	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting S
CVE-2019-25543	Netartmedia Real Estate Portal 5.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL c
CVE-2019-25527	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting S
CVE-2019-25509	XooDigital Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'p
CVE-2019-25528	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting S
CVE-2019-25530	uHotelBooking System contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through
CVE-2019-25510	Jettweb PHP Hazir Haber Sitesi Scripti V2 contains an authentication bypass vulnerability in the administration panel that allows unauthenticated attackers to gain a
CVE-2019-25512	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows attackers to inject malicious SQL commands through the kelime parame
CVE-2019-25531	Netartmedia Deals Portal contains an SQL injection vulnerability in the Email parameter of loginaction.php that allows unauthenticated attackers to manipulate dat
CVE-2019-25513	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting
CVE-2019-25514	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows attackers to inject malicious SQL commands through the kelime parame
CVE-2019-25488	Jettweb Hazir Rent A Car Scripti V4 contains multiple SQL injection vulnerabilities in the admin panel that allow unauthenticated attackers to manipulate database
CVE-2019-25482	Jettweb PHP Hazir Rent A Car Sitesi Scripti V2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injec
CVE-2019-25525	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting S
CVE-2019-25524	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the '
CVE-2019-25516	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting
CVE-2019-	iScripts ReserveLogic contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through t

25481	
CVE-2019-25532	Netartmedia Jobs Portal 6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code thr
CVE-2019-25479	Inout RealEstate contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the ci
CVE-2019-25533	Netartmedia PHP Business Directory 4.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting S
CVE-2019-25486	Varient 1.6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the user_
CVE-2015-20121	Next Click Ventures RealtyScript 4.0.2 contains SQL injection vulnerabilities that allow unauthenticated attackers to manipulate database queries by injecting arbit
CVE-2019-25517	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting
CVE-2019-25518	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting
CVE-2026-32231	ZeptoClaw is a personal AI assistant. Prior to 0.7.6, the generic webhook channel trusts caller-supplied identity fields (sender, chat_id) from the request body and a
CVE-2019-25519	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting malicious SQL co
CVE-2015-20120	Next Click Ventures RealtyScript 4.0.2 contains multiple time-based blind SQL injection vulnerabilities that allow unauthenticated attackers to extract database info
CVE-2019-25523	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the c
CVE-2019-25511	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting
CVE-2026-25529	Postal is an open source SMTP server. Postal versions less than 3.3.5 had a HTML injection vulnerability that allowed unescaped data to be included in the admin in
CVE-2026-32302	OpenClaw is a personal AI assistant. Prior to 2026.3.11, browser-originated WebSocket connections could bypass origin validation when gateway.auth.mode was se
CVE-2025-67298	An issue in ClasroomIO before v.0.2.6 allows a remote attacker to escalate privileges via the endpoints /api/verify and /rest/v1/profile
CVE-2026-32841	Edimax GS-5008PL firmware version 1.00.54 and prior contain an authentication bypass vulnerability that allows unauthenticated attackers to access the manager
CVE-2026-32247	Graphiti is a framework for building and querying temporal context graphs for AI agents. Graphiti versions before 0.28.2 contained a Cypher injection vulnerability search_nodes with attacker-controlled entity_types values. The MCP server mapped entity_types to SearchFilters.node_labels, which then reached the vulnerable C
CVE-2026-32116	Magic Wormhole makes it possible to get arbitrary-sized files and directories from one computer to another. From 0.21.0 to before 0.23.0, receiving a file (wormhol
CVE-2026-21361	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vvulnera a victim must browse to the page containing the vulnerable field.
CVE-2026-3453	The ProfilePress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.16.11. This is due to missing ownershi cancel and expire any other user's active subscription via the change_plan_sub_id parameter during checkout, causing immediate loss of paid access for victims.
CVE-2026-30911	Apache Airflow versions 3.1.0 through 3.1.7 missing authorization vulnerability in the Execution API's Human-in-the-Loop (HITL) endpoints that allows any authentic
CVE-2026-	The divi-booster WordPress plugin before 5.0.2 does not have authorization and CSRF checks in one of its fixing function, allowing unauthenticated users to modify

2626	
CVE-2026-24901	Outline is a service that allows for collaborative documentation. Prior to 1.4.0, an Insecure Direct Object Reference (IDOR) vulnerability in the document restoration
CVE-2026-32260	Deno is a JavaScript, TypeScript, and WebAssembly runtime. From 2.7.0 to 2.7.1, A command injection vulnerability exists in Deno's node:child_process polyfill (she execute. An attacker who controls arguments passed to spawnSync or spawn with shell: true can execute arbitrary OS commands, bypassing Deno's permission sy
CVE-2026-22202	wpDiscuz before 7.6.47 contains a cross-site request forgery vulnerability that allows attackers to delete all comments associated with an email address by crafting
CVE-2026-22193	wpDiscuz before 7.6.47 contains an SQL injection vulnerability in the getAllSubscriptions() function where string parameters lack proper quote escaping in SQL que
CVE-2026-21284	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab victim must browse to the page containing the vulnerable field.
CVE-2026-31892	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. From 2.9.0 to before 4.0.2 and 3.7.11, A user wh over the referenced WorkflowTemplate during spec merging and is applied directly to the pod spec at creation time with no security validation. This vulnerability is
CVE-2026-32729	Runtipi is a personal homeserver orchestrator. Prior to 4.8.1, The Runtipi /api/auth/verify-totp endpoint does not enforce any rate limiting, attempt counting, or acc practical request rates (~500 req/s), the attack completes in approximately 33 minutes in the worst case. This vulnerability is fixed in 4.8.1.
CVE-2026-21311	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab victim must browse to the page containing the vulnerable field.
CVE-2026-22248	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. From 11.0.0 t
CVE-2026-0956	There is a memory corruption vulnerability due to an out-of-bounds read when loading a corrupted file in Digilent DASYLab. This vulnerability may result in informa
CVE-2026-30902	Improper Privilege Management in certain Zoom Clients for Windows may allow an authenticated user to conduct an escalation of privilege via local access.
CVE-2017-20218	Serviio PRO 1.8 contains an unquoted search path vulnerability in the Windows service that allows local users to execute arbitrary code with elevated privileges by
CVE-2026-23862	Dell ThinOS 10 versions prior to ThinOS 2602_10.0573, contain an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerab
CVE-2026-32708	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, the Zenoh uORB subscriber allocates a stack VLA directly from the incoming payload length
CVE-2026-27940	llama.cpp is an inference of several LLM models in C/C++. Prior to b8146, the gguf_init_from_file_impl() in gguf.cpp is vulnerable to an Integer overflow, leading to
CVE-2026-0954	There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted DSB file in Digilent DASYLab. This vulnerability may result in in
CVE-2025-69783	A local attacker can bypass OpenEDR's 2.5.1.0 self-defense mechanism by renaming a malicious executable to match a trusted process name (e.g., csrss.exe, edrs privilege escalation.
CVE-2026-3888	Local privilege escalation in snapd on Linux allows local attackers to get root privilege by re-creating snap's private /tmp directory when systemd-tmpfiles is config
CVE-2026-0955	There is a memory corruption vulnerability due to an out-of-bounds read when loading a corrupted file in Digilent DASYLab. This vulnerability may result in informa
CVE-2025-64301	An out-of-bounds write vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2024-14026	A command injection vulnerability has been reported to affect several QNAP operating system versions. If an attacker gains local network access who have also ga
CVE-2026-3476	A Code Injection vulnerability affecting SOLIDWORKS Desktop from Release 2025 through Release 2026 could allow an attacker to execute arbitrary code on the us

CVE-2016-20033	Wowza Streaming Engine 4.5.0 contains a local privilege escalation vulnerability that allows authenticated users to escalate privileges by replacing executable files
CVE-2025-66342	A type confusion vulnerability exists in the EMF functionality of Canva Affinity. A specially crafted EMF file can trigger this vulnerability, which can lead to memory c
CVE-2026-4295	Improper trust boundary enforcement in Kiro IDE before version 0.8.0 on all supported platforms might allow a remote unauthenticated threat actor to execute arb
CVE-2026-3989	SGLangs `replay_request_dump.py` contains an insecure pickle.load() without validation and proper deserialization. An attacker can take advantage of this by prov
CVE-2026-0957	There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted file in Digilent DASYLab. This vulnerability may result in inform
CVE-2026-30900	Improper Check of minimum version in update functionality of certain Zoom Clients for Windows may allow an authenticated user to conduct an escalation of privil
CVE-2026-31881	Runtipi is a personal homeserver orchestrator. Prior to 4.8.0, an unauthenticated attacker can reset the operator (admin) password when a password-reset request
CVE-2026-32121	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, Stored XSS in prescription CSS/HTML trigger actions, and require independent fixes. This vulnerability is fixed in 8.0.0.1.
CVE-2026-32131	ZITADEL is an open source identity management platform. Prior to 3.4.8 and 4.12.2, a vulnerability in Zitadel's Management API has been reported, which allowed
CVE-2026-28521	arduino-TuyaOpen before version 1.2.1 contains an out-of-bounds memory read vulnerability in the TuyaIoT component. An attacker who hijacks or controls the Tu
CVE-2026-21670	A vulnerability allowing a low-privileged user to extract saved SSH credentials.
CVE-2026-32123	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, sensitivity checks for group encounte
CVE-2026-21887	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 6.8.16, the OpenCTI platform’s data ingestion featu in 6.8.16.
CVE-2026-32458	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 WOLF bulk-editor allows Blind SQL Injection.This
CVE-2026-32418	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jordy Meow Meow Gallery meow-gallery allows Blind SQL Inje
CVE-2026-31944	LibreChat is a ChatGPT clone with additional features. From 0.8.2 to 0.8.2-rc3, The MCP (Model Context Protocol) OAuth callback endpoint accepts the redirect from MCP-linked services (e.g. Atlassian, Outlook). This vulnerability is fixed in 0.8.3-rc1.
CVE-2026-32117	The grafanacubism-panel plugin allows use of cubism.js in Grafana. In 0.1.2 and earlier, the panel's zoom-link handler passes a dashboard-editor-supplied URL dire
CVE-2026-32101	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.3.1, the S3 storage manager's isAuthorized() function is declar
CVE-2026-32308	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.23, the Markdown viewer component renders Mermaid diagrams with securityLe
CVE-2026-32358	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdevelop Booking Calendar booking allows Blind SQL Injec
CVE-2026-2476	Mattermost Plugins versions <=2.0.3.0 fail to properly mask sensitive configuration values which allows an attacker with access to support packets to obtain origin
CVE-2026-32597	PyJWT is a JSON Web Token implementation in Python. Prior to 2.12.0, PyJWT does not validate the crit (Critical) Header Parameter defined in RFC 7515 §4.1.11. Wh
CVE-	

2026-3045	The Appointment Booking Calendar — Simply Schedule Appointments plugin for WordPress is vulnerable to unauthorized access of sensitive data in all versions up `remove_unauthorized_settings_for_current_user()` to filter restricted fields. This makes it possible for unauthenticated attackers to access admin-only plugin setti
CVE-2026-32130	ZITADEL is an open source identity management platform. From 2.68.0 to before 3.4.8 and 4.12.2, Zitadel provides a System for Cross-domain Identity Manageme manipulating data, an attacker could not modify or delete any user data. This vulnerability is fixed in 3.4.8 and 4.12.2.
CVE-2026-32426	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in themelexus Medilazar Core medilazar-cor
CVE-2026-3924	use after free in WindowDialog in Google Chrome prior to 146.0.7680.71 allowed a remote attacker who had compromised the renderer process to potentially perf
CVE-2026-32098	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.9 and 8.6.35, an attacker can exploit L configured in Class-Level Permissions and LiveQuery enabled. This vulnerability is fixed in 9.6.0-alpha.9 and 8.6.35.
CVE-2026-32400	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemetechMount Boldman boldman allow
CVE-2026-32393	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Creatives_Planet Greenly Theme Addons g
CVE-2026-22182	wpDiscuz before 7.6.47 contains an unauthenticated denial of service vulnerability that allows anonymous users to trigger mass notification emails by exploiting th
CVE-2026-31882	Dagu is a workflow engine with a built-in Web user interface. Prior to 2.2.4, when Dagu is configured with HTTP Basic authentication (DAGU_AUTH_MODE=basic), a an auth.Options struct with BasicAuthEnabled: true but AuthRequired defaults to false (Go zero value). The authentication middleware at internal/service/frontend/
CVE-2026-32392	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Creatives_Planet Greenly greenly allows P
CVE-2026-2890	The Formidable Forms plugin for WordPress is vulnerable to a payment integrity bypass in all versions up to, and including, 6.28. This is due to the Stripe Link retur reuse a PaymentIntent from a completed low-value payment to mark a high-value payment as complete, effectively bypassing payment for goods or services.
CVE-2026-32384	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in magepeopleteam WpBookingly service-bo
CVE-2026-32369	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RadiusTheme Medilink-Core medilink-core
CVE-2026-32364	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in redqteam Turbo Manager turbo-manager
CVE-2019-25515	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an authentication bypass vulnerability in the login.php administration panel that allows unauthenticated attacker
CVE-2026-25819	HMS Networks Ewon Flexy with firmware before 15.0s4, Cosy+ with firmware 22.xx before 22.1s6, and Cosy+ with firmware 23.xx before 23.0s3 allows unauthenti
CVE-2026-32319	Ella Core is a 5G core designed for private networks. Prior to 1.5.1, Ella Core panics when processing a malformed integrity protected NGAP/NAS message with a le
CVE-2026-3657	The My Sticky Bar plugin for WordPress is vulnerable to SQL injection via the `stickymenu_contact_lead_form` AJAX action in all versions up to, and including, 2.8.6 based data extraction from the database.
CVE-2026-31899	CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to Kozea/CairoSVG has exponential denial of service via recursive <use> element amplifi
CVE-2026-2673	Issue summary: An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group configuration includes server. If an OpenSSL TLS 1.3 server's configuration uses the 'DEFAULT' keyword to interpolate the built-in default group list into its own configuration, perhaps add quantum key agreement group, such as 'X25519MLKEM768', if the client's configuration results in only 'classical' groups (such as 'X25519' being the only ones in t supported by the client, but not included in the list of predicted keyshares would have been more preferred, if included. The new syntax partitions the groups into above works as expected when the server's configuration uses the built-in default group list, or explicitly defines its own list by directly defining the various desired
CVE-2026-3932	Insufficient policy enforcement in PDF in Google Chrome on Android prior to 146.0.7680.71 allowed a remote attacker to bypass navigation restrictions via a crafte
CVE-2026-	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to properly handle very long passwords, which allows an attacker to overload th

24458	
CVE-2026-3222	The WP Maps plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'location_id' parameter in all versions up to, and including, 4.9.1. This is d `location_id` GET parameter directly to a database query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existi
CVE-2025-69768	SQL Injection vulnerability in Chyrp v.2.5.2 and before allows a remote attacker to obtain sensitive information via the Admin.php component
CVE-2026-32295	JetKVM before 0.5.4 does not rate limit login requests, enabling brute-force attempts to guess credentials.
CVE-2026-32614	Go ShangMi (Commercial Cryptography) Library (GMSM) is a cryptographic library that covers the Chinese commercial cryptographic public algorithms SM2/SM3/SM infinity, causing the bilinear pairing result to degenerate into the identity element in the GT group. As a result, a critical part of the key derivation input becomes a
CVE-2026-1528	ImpactA server can reply with a WebSocket frame using the 64-bit length form and an extremely large length. undici's ByteParser overflows internal math, ends up
CVE-2026-32292	The GL-iNet Comet (GL-RM1) KVM web interface does not limit login requests, enabling brute-force attempts to guess credentials.
CVE-2026-28779	Apache Airflow versions 3.1.0 through 3.1.7 session token (_token) in cookies is set to path=/ regardless of the configured [webserver] base_url or [api] base_url. T
CVE-2026-4258	All versions of the package sjcl are vulnerable to Improper Verification of Cryptographic Signature due to missing point-on-curve validation in sjcl.ecc.basicKey.pub
CVE-2026-3805	When doing a second SMB request to the same host again, curl would wrongly use a data pointer pointing into already freed memory.
CVE-2026-2579	The WowStore – Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the ‘search’ parameter in all versions up t
CVE-2026-31958	Tornado is a Python web framework and asynchronous networking library. In versions of Tornado prior to 6.5.5, the only limit on the number of parts in multipart/fo
CVE-2026-2413	The Ally – Web Accessibility & Usability plugin for WordPress is vulnerable to SQL Injection via the URL path in all versions up to, and including, 4.0.3. This is due to SQL queries into already existing queries that can be used to extract sensitive information from the database via time-based blind SQL injection techniques. The Re
CVE-2026-28356	multipart is a fast multipart/form-data parser for python. Prior to 1.2.2, 1.3.1 and 1.4.0-dev, the parse_options_header() function in multipart.py uses a regular expr
CVE-2026-4276	LibreChat RAG API, version 0.7.0, contains a log-injection vulnerability that allows attackers to forge log entries.
CVE-2026-21888	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. MQTT v5 Variable Byte Integer parsing out-of-bounds: get_var_integer() accepts 5-byte
CVE-2026-32062	OpenClaw versions2026.2.21-2 prior to 2026.2.22 and @openclaw/voice-call versions 2026.2.21 prior to 2026.2.22 accept media-stream WebSocket upgrades befo
CVE-2026-30405	An issue in GoBGP gobgpd v.4.2.0 allows a remote attacker to cause a denial of service via the NEXT_HOP path attribute
CVE-2026-1069	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.9 before 18.9.2 that could have allowed an unauthenticated user to cause a denial of
CVE-2026-3496	The JetBooking plugin for WordPress is vulnerable to SQL Injection via the 'check_in_date' parameter in all versions up to, and including, 4.0.3. This is due to insuffi
CVE-2025-14513	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.11 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed
CVE-2025-13929	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.0 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that

21309	
CVE-2025-70027	An issue pertaining to CWE-918: Server-Side Request Forgery was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4. This allows attackers to obtain sensitive infor
CVE-2026-2229	ImpactThe undici WebSocket client is vulnerable to a denial-of-service attack due to improper validation of the server_max_window_bits parameter in the permessa causing a synchronous RangeError exception that is not caught, resulting in immediate process termination. The vulnerability exists because: * The isValidClientWi
CVE-2025-66687	Doom Launcher 3.8.1.0 is vulnerable to Directory Traversal due to missing file path validation during the extraction of game files
CVE-2026-21289	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2026-4269	A missing S3 ownership verification in the Bedrock AgentCore Starter Toolkit before version v0.1.13 may allow a remote actor to inject code during the build proces v0.1.13.
CVE-2026-30226	Svelte devalue is a JavaScript library that serializes values into strings when JSON.stringify isn't sufficient for the job. In devalue v5.6.3 and earlier, devalue.parse a
CVE-2026-1708	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to blind SQL Injection in all versions up to, the database via the `append_where_sql` parameter in JSON payloads granted they have obtained a valid `public_token` that is inadvertently exposed during the l
CVE-2026-31866	flagd is a feature flag daemon with a Unix philosophy. Prior to 0.14.2, flagd exposes OFREP (/ofrep/v1/evaluate/...) and gRPC (evaluation.v1, evaluation.v2) endpoin termination (e.g., OOMKill in Kubernetes environments). flagd does not natively enforce authentication on its evaluation endpoints. While operators may deploy fla
CVE-2026-1376	IBM i 7.6 could allow a remote attacker to cause a denial of service using failed authentication connections due to improper allocation of resources.
CVE-2026-4111	A flaw was identified in the RAR5 archive decompression logic of the libarchive library, specifically within the archive_read_data() processing path. When a specially service conditions in services that automatically process archives.
CVE-2026-31894	WeGIA is a web manager for charitable institutions. In 3.6.5, The patched loadBackupDB() extracts tar.gz archives to a temporary directory using PHP's PharData cl
CVE-2026-27703	RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. In 2 service or arbitrary code execution.
CVE-2013-20006	Qool CMS contains multiple persistent cross-site scripting vulnerabilities in several administrative scripts where POST parameters are not properly sanitized before
CVE-2026-22727	Unprotected internal endpoints in Cloud Foundry Capi Release 1.226.0 and below, and CF Deployment v54.9.0 and below on all platforms allows any user who has
CVE-2025-14031	IBM Sterling B2B Integrator and and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1, and 6.2.2.0 could all
CVE-2026-31887	Shopware is an open commerce platform. Prior to 6.7.8.1 and 6.6.10.15, an insufficient check on the filter types for unauthenticated customers allows access to or
CVE-2025-70873	An information disclosure issue in the zipfileInflate function in the zipfile extension in SQLite v3.51.1 and earlier allows attackers to obtain heap memory via supply
CVE-2019-25480	ARMBot contains an unrestricted file upload vulnerability in upload.php that allows unauthenticated attackers to upload arbitrary files by manipulating the file para
CVE-2019-25478	GetGo Download Manager 6.2.2.3300 contains a buffer overflow vulnerability that allows remote attackers to cause denial of service by sending HTTP responses w
CVE-2026-32838	Edimax GS-5008PL firmware version 1.00.54 and prior use cleartext HTTP for the web management interface without implementing TLS or SSL encryption. Attacke
CVE-2017-20217	Serviio PRO 1.8 contains an information disclosure vulnerability due to improper access control enforcement in the Configuration REST API that allows unauthentica
CVE-2026-	The Angeet ES3 KVM allows a remote, unauthenticated attacker to write arbitrary files, including configuration files or system binaries. Modified configuration files

32297	
CVE-2026-32141	flatted is a circular JSON parser. Prior to 3.4.0, flatted's parse() function uses a recursive revive() phase to resolve circular references in deserialized JSON. When gi
CVE-2017-20220	Serviio PRO 1.8 contains an improper access control vulnerability in the Configuration REST API that allows unauthenticated attackers to change the mediabrowser
CVE-2019-25472	IntelBras Telefone IP TIP200 and 200 LITE contain an unauthenticated arbitrary file read vulnerability in the dumpConfigFile function accessible via the cgiServer.ex
CVE-2026-32981	A path traversal vulnerability was identified in Ray Dashboard (default port 8265) in Ray versions prior to 2.8.1. Due to improper validation and sanitization of user-
CVE-2026-1526	The undici WebSocket client is vulnerable to a denial-of-service attack via unbounded memory consumption during permessage-deflate decompression. When a W unresponsive. The vulnerability exists in the PerMessageDeflate.decompress() method, which accumulates all decompressed chunks in memory and concatenates
CVE-2019-25470	eWON Firmware versions 12.2 to 13.0 contain an authentication bypass vulnerability that allows attackers with minimal privileges to retrieve sensitive user data by
CVE-2017-20222	Telesquare SKT LTE Router SDT-CS3B1 software version 1.2.0 contains an unauthenticated remote reboot vulnerability that allows attackers to trigger device reboo
CVE-2019-25465	Hisilicon Hilpcam V100R003 contains a directory traversal vulnerability that allows unauthenticated attackers to access sensitive configuration files by exploiting d
CVE-2026-31872	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.6 and 8.6.32, the protectedFields class
CVE-2026-31870	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.37.1, when a cpp-httplib client uses the streaming API (httplib::stream:: SIGABRT. Any server the client connects to — including servers reached via HTTP redirects, third-party APIs, or man-in-the-middle positions can crash the client app
CVE-2026-1947	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 9.
CVE-2026-28498	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.9, a library-level vulnerability was identified in the Authlib Python lib supplying a forged ID Token with a deliberately unrecognized alg header parameter. The library intercepts the unsupported state and silently returns True (validati
CVE-2025-71263	In UNIX Fourth Research Edition (v4), the su command is vulnerable to a buffer overflow due to the 'password' variable having a fixed size of 100 bytes. A local use
CVE-2026-32242	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.11 and 8.6.37, Parse Server's built-in C policy. Deployments that configure multiple OAuth2 providers via the oauth2: true flag are affected. This vulnerability is fixed in 9.6.0-alpha.11 and 8.6.37.
CVE-2026-32775	libexif through 0.6.25 has a flaw in decoding MakerNotes. If the exif_mnote_data_get_value function gets passed in a 0 size, the passed in-buffer would be overwrit
CVE-2026-32132	ZITADEL is an open source identity management platform. Prior to 3.4.8 and 4.12.2, a potential vulnerability exists in Zitadel's passkey registration endpoints. This
CVE-2026-28791	Tina is a headless content management system. Prior to 2.1.7, a path traversal vulnerability exists in the TinaCMS development server's media upload handler. The
CVE-2026-20074	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) multi-instance routing feature of Cisco IOS XR Software could allow an unauthenticated, a to advertised networks and a denial of service (DoS) condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer
CVE-2026-3980	A vulnerability has been found in itsourcecode Online Doctor Appointment System 1.0. This impacts an unknown function of the file /admin/patient_action.php. Suc
CVE-2026-4237	A flaw has been found in itsourcecode Free Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /hotel/admin/mod_reports/index.php. E
CVE-2026-4319	A vulnerability was identified in code-projects Simple Food Order System 1.0. Affected by this vulnerability is an unknown functionality of the file /routers/add-item.
CVE-2026-4014	A security flaw has been discovered in itsourcecode Cafe Reservation System 1.0. This impacts an unknown function of the file /curvus2/signup.php of the compone

CVE-2026-4232	A vulnerability was determined in Tiandy Integrated Management Platform 7.17.0. Affected by this issue is some unknown functionality of the file /rest/user/getAut
CVE-2026-4235	A weakness has been identified in itsourcecode Online Enrollment System 1.0. This issue affects some unknown processing of the file /sms/login.php. This manipul
CVE-2026-4236	A security vulnerability has been detected in itsourcecode Online Enrollment System 1.0. Impacted is an unknown function of the file /enrollment/index.php?view=
CVE-2026-3969	A vulnerability was detected in FeMiner wms up to 1.0. This impacts an unknown function of the file /wms-master/src/basic/depart/depart_add_bg.php of the compo
CVE-2026-25076	Anchore Enterprise versions before 5.25.1 contain an SQL injection vulnerability in the GraphQL Reports API. An authenticated attacker that is able to access the G
CVE-2026-3981	A vulnerability was found in itsourcecode Online Doctor Appointment System 1.0. Affected is an unknown function of the file /admin/doctor_action.php. Performing
CVE-2026-4231	A vulnerability was found in vanna-ai vanna up to 2.0.2. Affected by this vulnerability is the function update_sql/run_sql of the file src/vanna/legacy/flask/__init__.py
CVE-2026-4288	A weakness has been identified in Tiandy Easy7 Integrated Management Platform 7.17.0. The impacted element is an unknown function of the file /rest/devStatus/
CVE-2026-4287	A security flaw has been discovered in Tiandy Easy7 Integrated Management Platform 7.17.0. The affected element is an unknown function of the file /rest/devStat
CVE-2026-4289	A security vulnerability has been detected in Tiandy Easy7 Integrated Management Platform up to 7.17.0. This affects an unknown function of the file /rest/preSetT
CVE-2026-3943	A vulnerability was found in H3C ACG1000-AK230 up to 20260227. This affects an unknown part of the file /webui/?aaa_portal_auth_local_submit. The manipulation
CVE-2026-4229	A flaw has been found in vanna-ai vanna up to 2.0.2. This impacts the function remove_training_data of the file src/vanna/legacy/google/bigquery_vector.py. This m
CVE-2026-4180	A vulnerability was identified in D-Link DIR-816 1.10CNB05. The impacted element is an unknown function of the file redirect.asp of the component goahead. The m
CVE-2026-4194	A vulnerability was detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-3
CVE-2026-4221	A vulnerability was found in Tiandy Easy7 Integrated Management Platform 7.17.0. This affects an unknown part of the file /rest/file/uploadLedImage of the compon
CVE-2026-4200	A security flaw has been discovered in glowxq glowxq-oj up to 6f7c723090472057252040fd2bbbdaa1b5ed2393. This affects the function uploadTestcaseZipUrl of t available. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-4220	A vulnerability has been found in Technologies Integrated Management Platform 7.17.0. Affected by this issue is some unknown functionality of the file /SetWebpag
CVE-2026-4191	A flaw has been found in JawherKl node-api-postgres up to 2.5. Affected is the function path.extname of the file index.js of the component Profile Picture Handler. T
CVE-2026-32594	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.40 and 9.6.0-alpha.14, the GraphQL WebSocke arbitrarily complex queries that bypass configured complexity limits. This vulnerability is fixed in 8.6.40 and 9.6.0-alpha.14.
CVE-2026-4201	A weakness has been identified in glowxq glowxq-oj up to 6f7c723090472057252040fd2bbbdaa1b5ed2393. This vulnerability affects the function Upload of the file contacted early about this disclosure but did not respond in any way.
CVE-2026-4190	A vulnerability was detected in JawherKl node-api-postgres up to 2.5. This impacts the function User.getAll of the file models/user.js. The manipulation of the argum
CVE-2026-4193	A security vulnerability has been detected in D-Link DIR-823G 1.0.2B05. The affected element is the function GetDDNSSettings/GetDeviceDomainName/GetDeviceSettings/GetDMZSettings/GetFirewallSettings/GetGuestNetworkSettings/GetLanWanConflictInfo/GetLocalMacA of the component goahead. Such manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed publicly ar

CVE-2026-3944	A vulnerability was determined in itsourcecode University Management System 1.0. This vulnerability affects unknown code of the file /att_add.php. This manipulat
CVE-2026-4223	A vulnerability was identified in itsourcecode Payroll Management System 1.0. This issue affects some unknown processing of the file /manage_employee.php. Suc
CVE-2026-32414	Improper Control of Generation of Code ('Code Injection') vulnerability in ILLID Advanced Woo Labels advanced-woo-labels allows Remote Code Inclusion.This issue
CVE-2026-4172	A vulnerability was detected in TRENDnet TEW-632BRP 1.010B32. This affects an unknown part of the file /ping_response.cgi of the component HTTP POST Reques
CVE-2026-23759	Perle IOLAN STS/SCS terminal server models with firmware versions prior to 6.0 allow authenticated OS command injection via the restricted shell accessed over Te
CVE-2026-20163	In Splunk Enterprise versions below 10.2.0, 10.0.4, 9.4.9, and 9.3.10, and Splunk Cloud Platform versions below 10.2.2510.5, 10.0.2503.12, 10.1.2507.16, and 9.3.1
CVE-2016-20032	ZKTeco ZKAccess Security System 5.3.1 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary HTML and script code by injec
CVE-2015-20118	Next Click Ventures RealtyScript 4.0.2 contains a stored cross-site scripting vulnerability in the location_name parameter of the admin locations interface. Attacker
CVE-2015-20115	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize file uploads, allowing attackers to store malicious scripts through the file POST parameter in admin/t
CVE-2026-32263	Craft CMS is a content management system (CMS). From version 5.6.0 to before version 5.9.11, in src/controllers/EntryTypesController.php, the $settings array fro
CVE-2026-32264	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.5 and from version 5.0.0-RC1 to before version 5.9.11, there is a
CVE-2026-3873	Use of Hard-coded Credentials vulnerability in Avantra allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Avantra: before 25.3.0.
CVE-2026-3231	The Checkout Field Editor (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom radio and checkboxg allowlist in `get_allowed_html()` that explicitly permits the `<select>` element with the `onchange` event handler attribute. This makes it possible for unauthentic
CVE-2026-3178	The Name Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name_directory_name' parameter in all versions up to, and including,
CVE-2026-23815	A vulnerability in a custom binary used in AOS-CX Switches' CLI could allow an authenticated remote attacker with high privileges to perform command injection. S
CVE-2026-23816	A vulnerability in the command line interface of AOS-CX Switches could allow an authenticated remote attacker to execute arbitrary commands on the underlying o
CVE-2026-32401	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in BoldGrid Client Invoicing by Sprout Invoice
CVE-2026-1454	The Responsive Contact Form Builder & Lead Generation Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including administrator views the lead entries in the WordPress dashboard.
CVE-2019-25473	Clinic Pro contains a SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the month paran
CVE-2026-26133	AI command injection in M365 Copilot allows an unauthorized attacker to disclose information over a network.
CVE-2026-32126	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, an inverted boolean condition in Cont configurations — all operations intended to require administrator privileges. This vulnerability is fixed in 8.0.0.1.
CVE-2026-25369	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Flexmls Flexmls® IDX allows Reflected XSS.This issue affects F

CVE-2026-32617	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, On default installa is only viable from within the same local network (LAN) due to browser-level blocking of public-to-private requests.
CVE-2026-1715	An input validation vulnerability was reported in the DeviceSettingsSystemAddin used in Lenovo Vantage and Lenovo Baiying that could allow a local authenticated
CVE-2026-1716	An input validation vulnerability was reported in the DeviceSettingsSystemAddin used in Lenovo Vantage and Lenovo Baiying that could allow a local authenticated
CVE-2019-25529	Placeto CMS Alpha rv.4 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through th
CVE-2026-2466	The DukaPress WordPress plugin through 3.2.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Sc
CVE-2026-32706	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, The crsf_rc parser accepts an oversized variable-length known packet and copies it into a fix
CVE-2026-1264	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1, and 6.2.2.0 allows a remo
CVE-2026-32063	OpenClaw version 2026.2.19-2 prior to 2026.2.21 contains a command injection vulnerability in systemd unit file generation where attacker-controlled environmen
CVE-2026-2368	An improper certificate validation vulnerability was reported in the Lenovo Filez application that could allow a user capable of intercepting network traffic to execut
CVE-2026-30901	Improper Input Validation in Zoom Rooms for Windows before 6.6.5 in Kiosk Mode may allow an authenticated user to conduct an escalation of privilege via local ac
CVE-2026-2808	HashiCorp Consul and Consul Enterprise 1.18.20 up to 1.21.10 and 1.22.4 are vulnerable to arbitrary file read when configured with Kubernetes authentication. Thi
CVE-2026-32229	In JetBrains Hub before 2026.1 possible on sign-in account mismatch with non-SSO auth and 2FA disabled
CVE-2026-32103	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.3, the POST /studiocms_api/dashboard/create-reset-link endp takeover of the highest-privileged account in the system. This vulnerability is fixed in 0.4.3.
CVE-2026-32112	ha-mcp is a Home Assistant MCP Server. Prior to 7.0.0, the ha-mcp OAuth consent form renders user-controlled parameters via Python f-strings with no HTML escap
CVE-2026-20118	A vulnerability in the handling of an Egress Packet Network Interface (EPNI) Aligner interrupt in Cisco IOS XR Software for Cisco Network Convergence System (NCS affected device is experiencing heavy transit traffic. An attacker could exploit this vulnerability by sending a continuous flow of crafted packets to an interface of th score indicates. This change was made because the affected device operates within a critical network segment where compromise could lead to significant disrupt
CVE-2026-1753	The Gutena Forms WordPress plugin before 1.6.1 does not validate option to be updated, which could allow contributors and above role to update arbitrary boolean
CVE-2026-32705	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, the BST telemetry probe writes a string terminator using a device-provided length without bo
CVE-2026-31864	JumpServer is an open source bastion host and an operation and maintenance security audit system. a Server-Side Template Injection (SSTI) vulnerability exists in uploaded YAML configuration files. When a user uploads an Applet or VirtualApp ZIP package, the manifest.yml file is rendered through Jinja2 without sandbox restr
CVE-2026-21360	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Improper Limitation of a Pathname to a R
CVE-2026-32291	The GL-iNet Comet (GL-RM1) KVM does not require authentication on the UART serial console. This attack requires physically opening the device and connecting to
CVE-2026-32259	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-16 and 6.9.13-41, when a memory allocation fails in
CVE-2026-4105	A flaw was found in systemd. The systemd-machined service contains an Improper Access Control vulnerability due to insufficient validation of the class parameter

CVE-2026-0940	A potential improper initialization vulnerability was reported in the BIOS of some ThinkPads that could allow a local privileged user to modify data and execute arbi
CVE-2024-14025	An SQL injection vulnerability has been reported to affect Video Station. If an attacker gains local network access who have also gained an administrator account, t
CVE-2026-24510	Dell Alienware Command Center (AWCC), versions prior to 6.12.24.0, contain an Improper Privilege Management vulnerability. A low privileged attacker with local a
CVE-2024-14024	An improper certificate validation vulnerability has been reported to affect Video Station. If an attacker gains local network access who have also gained an admini
CVE-2026-2462	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to restrict plugin installation on CI test instances with default admin credentials
CVE-2025-13778	Missing authentication for critical function vulnerability in ABB AWIN GW100 rev.2, ABB AWIN GW120.This issue affects AWIN GW100 rev.2: 2.0-0, 2.0-1; AWIN GW1
CVE-2026-28803	Open Forms allows users create and publish smart forms. Prior to 3.3.13 and 3.4.5, to be able to cosign, the cosigner receives an e-mail with instructions or a deep
CVE-2026-30234	OpenProject is an open-source, web-based project management software. Prior to 17.2.0, an authenticated project member with BCF import permissions can uploa read permissions of the OpenProject application user. This vulnerability is fixed in 17.2.0.
CVE-2026-32704	SiYuan is a personal knowledge management system. Prior to 3.6.1, POST /api/template/renderSprig lacks model.CheckAdminRole, allowing any authenticated use
CVE-2026-20164	In Splunk Enterprise versions below 10.2.0, 10.0.3, 9.4.9, and 9.3.10, and Splunk Cloud Platform versions below 10.2.2510.5, 10.1.2507.16, 10.0.2503.11, and 9.3.
CVE-2026-30239	OpenProject is an open-source, web-based project management software. Prior to 17.2.0, when budgets are deleted, the work packages that were assigned to this
CVE-2026-30235	OpenProject is an open-source, web-based project management software. Prior to 17.2.0, this vulnerability occurs due to improper validation of OpenProject's Mark
CVE-2026-31841	Hyperterse is a tool-first MCP framework for building AI-ready backend surfaces from declarative config. Prior to v2.2.0, the search tool allows LLMs to search for to
CVE-2026-28522	arduino-TuyaOpen before version 1.2.1 contains a null pointer dereference vulnerability in the WiFiUDP component. An attacker on the same local area network ca
CVE-2025-12736	in OpenHarmony v5.0.3 and prior versions allow a local attacker case sensitive information leak through use of uninitialized resource.
CVE-2025-61154	Heap buffer overflow vulnerability in LibreDWG versions v0.13.3.7571 up to v0.13.3.7835 allows a crafted DWG file to cause a Denial of Service (DoS) via the funct
CVE-2026-32094	Shescape is a simple shell escape library for JavaScript. Prior to 2.1.10, Shescape#escape() does not escape square-bracket glob syntax for Bash, BusyBox sh, and
CVE-2026-32460	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Ultimate Addons for Contact Form 7 ultimate-addons
CVE-2025-13690	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.11 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed
CVE-2026-32598	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.24, the password reset flow logs the complete password reset URL — containing
CVE-2025-12576	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.3 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that under certain conditio
CVE-2026-1781	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 4.11.1. This is due to the plug exposed in the HTML source).

CVE-2026-32842	Edimax GS-5008PL firmware version 1.00.54 and prior contain an insecure credential storage vulnerability that allows attackers to obtain administrator credentials
CVE-2026-1267	IBM Planning Analytics Local 2.1.0 through 2.1.17 could allow an unauthorized access to sensitive application data and administrative functionalities due to lack of
CVE-2026-25936	GLPI is a free Asset and IT management software package. Starting in version 11.0.0 and prior to version 11.0.6, an authenticated user can perfom a SQL injection.
CVE-2026-4147	An authenticated user with the read role may read limited amounts of uninitialized stack memory via specially-crafted issuances of the filemd5 command.
CVE-2026-21886	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to version 6.9.1, the GraphQL mutations "IndividualD
CVE-2026-26929	Apache Airflow versions 3.0.0 through 3.1.7 FastAPI DagVersion listing API does not apply per-DAG authorization filtering when the request is made with dag_id set
CVE-2026-32245	Tinyauth is an authentication and authorization server. Prior to 5.0.3, the OIDC token endpoint does not verify that the client exchanging an authorization code is t
CVE-2026-3954	A weakness has been identified in OpenBMB XAgent 1.0.0. Affected by this vulnerability is the function workspace of the file XAgentServer/application/routers/work
CVE-2025-68971	In Forgejo through 13.0.3, the attachment component allows a denial of service by uploading a multi-gigabyte file attachment (e.g., to be associated with an issue
CVE-2026-28490	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.9, a cryptographic padding oracle vulnerability was identified in the
CVE-2026-1525	Undici allows duplicate HTTP Content-Length headers when they are provided in an array with case-variant names (e.g., Content-Length and content-length). This p with duplicate Content-Length headers (400 Bad Request) * HTTP Request Smuggling: In deployments where an intermediary and backend interpret duplicate head
CVE-2026-23817	A vulnerability in the web-based management interface of AOS-CX Switches could allow an unauthenticated remote attacker to redirect users to an arbitrary URL.
CVE-2026-32269	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.13 and 8.6.39, the OAuth2 authenticat data for the malformed request. Deployments using the OAuth2 adapter with appidField and appIds configured are affected. This vulnerability is fixed in 9.6.0-alph
CVE-2026-1965	libcurl can in some circumstances reuse the wrong connection when asked to do an Negotiate-authenticated HTTP or HTTPS request. libcurl features a pool of rece authenticates *connections* and not *requests*, contrary to how HTTP is designed to work. An application that allows Negotiate authentication to a server (that res when it is in fact still using the connection authenticated for user1... The set of authentication methods to use is set with `CURLOPT_HTTPAUTH`. Applications can c
CVE-2026-3784	curl would wrongly reuse an existing HTTP proxy connection doing CONNECT to a server, even if the new request uses different credentials for the HTTP proxy. The
CVE-2025-66955	Local File Inclusion in Contact Plan, E-Mail, SMS and Fax components in Asseco SEE Live 2.0 allows remote authenticated users to access files on the host via "path
CVE-2026-32455	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 MDTF wp-meta-data-filter-and-taxonomy-filter allo
CVE-2026-31918	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in immonex immonex Kickstart immonex-kickstart allows Stored
CVE-2026-32361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marketing Fire Editorial Calendar editorial-calendar allows DOM
CVE-2026-32359	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Icon List Block icon-list-block allows Stored XSS.This is
CVE-2026-32356	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in robosoft Robo Gallery robo-gallery allows DOM-Based XSS.This
CVE-2026-32352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows DOM-B
CVE-	

2026-32320	Ella Core is a 5G core designed for private networks. Prior to 1.5.1, Ella Core panics when processing a PathSwitchRequest containing UE Security Capabilities with
CVE-2026-31949	LibreChat is a ChatGPT clone with additional features. Prior to 0.8.3-rc1, a Denial of Service (DoS) vulnerability exists in the DELETE /api/convos endpoint that allow
CVE-2026-31885	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, there is an out-of-bounds read in MS-ADPCM and IMA-ADPCM decoders due to ur
CVE-2026-3934	Insufficient policy enforcement in ChromeDriver in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to bypass same origin policy via a crafted HTM
CVE-2026-31884	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, division by zero in MS-ADPCM and IMA-ADPCM decoders when nBlockAlign is 0, l vulnerability is fixed in 3.24.0.
CVE-2026-31883	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, a size_t underflow in the IMA-ADPCM and MS-ADPCM audio decoders leads to hea ~SIZE_MAX. The while (size > 0) loop then continues for an astronomical number of iterations. This vulnerability is fixed in 3.24.0.
CVE-2026-30955	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to 2.2.4, An API endpoint accepts unbounded request bodies with
CVE-2026-22216	wpDiscuz before 7.6.47 contains a missing rate limiting vulnerability that allows unauthenticated attackers to subscribe arbitrary email addresses to post notificati
CVE-2026-22191	wpDiscuz before 7.6.47 contains a shortcode injection vulnerability that allows attackers to execute arbitrary shortcodes by including them in comment content se
CVE-2025-36368	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, and 6.2.1.0 through 6.2.1.1_1 are vulnerable to SQL
CVE-2026-3935	Incorrect security UI in WebAppInstalls in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chrom
CVE-2026-3937	Incorrect security UI in Downloads in Google Chrome on Android prior to 146.0.7680.71 allowed a remote attacker to perform UI spoofing via a crafted HTML page.
CVE-2026-32443	Cross-Site Request Forgery (CSRF) vulnerability in Josh Kohlbach Product Feed PRO for WooCommerce woo-product-feed-pro allows Cross Site Request Forgery.This
CVE-2026-32454	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Avada Core fusion-core allows DOM-Based XSS.T
CVE-2026-32411	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simpma Embed Calendly embed-calendly-scheduling allows St
CVE-2026-32424	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Sprout Clients sprout-clients allows Stored XSS.This is
CVE-2026-32429	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Magical Addons For Elementor magical-addons-for-e
CVE-2026-32430	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IdeaBox Creations PowerPack Addons for Elementor powerpack
CVE-2026-32431	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Astra Bulk Edit astra-bulk-edit allows DOM-Ba
CVE-2026-32108	Copyparty is a portable file server. Prior to 1.20.12, there was a missing permission-check in the shares feature (the shr global-option). This vulnerability only appli not possible to descend into subdirectories in this manner; only the sibling files were accessible. This vulnerability is similar to CVE-2025-58753 which was previous
CVE-2026-32403	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in toocheke Toocheke Companion toocheke-companion allows DO
CVE-2026-32448	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric Teubert Podlove Podcast Publisher podlove-podcasting-plu
CVE-	

2026-32102	OliveTin gives access to predefined shell commands from a web interface. In 3000.10.2 and earlier, OliveTin's live EventStream broadcasts execution events and a
CVE-2026-32450	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-p
CVE-2026-32449	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Event Post themify-event-post allows Store
CVE-2026-2257	The GetGenie plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.2 due to missing validation on a user c
CVE-2026-3986	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form settings in all versions up to, and including, 5.4.5.0. This is
CVE-2026-4358	A specially crafted aggregation query with $lookup by an authenticated user with write privileges can cause a double-free or use-after-free memory issue in the slo
CVE-2026-32774	Vulnogram 1.0.0 contains a stored cross-site scripting vulnerability in comment hypertext handling that allows attackers to inject malicious scripts. Remote attacke
CVE-2015-20119	Next Click Ventures RealtyScript 4.0.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious HTML and iframe el
CVE-2026-32353	Server-Side Request Forgery (SSRF) vulnerability in MailerPress Team MailerPress mailerpress allows Server Side Request Forgery.This issue affects MailerPress: fro
CVE-2026-32357	Server-Side Request Forgery (SSRF) vulnerability in Katsushi Kawamori Simple Blog Card simple-blog-card allows Server Side Request Forgery.This issue affects Sir
CVE-2025-8766	A container privilege escalation flaw was found in certain Multi-Cloud Object Gateway Core images. This issue stems from the /etc/passwd file being created with g
CVE-2025-57849	A container privilege escalation flaw was found in certain Fuse images. This issue stems from the /etc/passwd file being created with group-writable permissions du
CVE-2026-2569	The Dear Flipbook – PDF Flipbook, 3D Flipbook, PDF embed, PDF viewer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via PDF page labels in all v
CVE-2026-3492	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.9.28.1. This is due to a compound failure i not quotes). This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary JavaScript that executes when an Admini
CVE-2026-2918	The Happy Addons for Elementor plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.21.0 via the `ha_cond the display conditions of any published `ha_library` template. Because the `cond_to_html()` renderer outputs condition values into HTML attributes without proper
CVE-2026-3534	The Astra theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `ast-page-background-meta` and `ast-content-background-meta` post meta fiel arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2026-2358	The WP ULike plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `[wp_ulike_likers_box]` shortcode `template` attribute in all versions up to, a must have at least one like for the XSS to render.
CVE-2026-2707	The weForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the REST API entry submission endpoint in all versions up to, and including, 1.6.2 base field handler only applies `trim()` to the value. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary w
CVE-2026-3977	A security vulnerability has been detected in projectsend up to r1945. The affected element is an unknown function of the component AJAX Endpoints. The manipul
CVE-2026-4192	A vulnerability has been found in AvinashBole quip-mcp-server 1.0.0. Affected by this vulnerability is the function setupToolHandlers of the file src/index.ts. Such m
CVE-2026-4195	A flaw has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, D
CVE-2026-4196	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS
CVE-	

2026-4197	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L The exploit has been made public and could be used.
CVE-2025-66249	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache Livy. This issue affects Apache Livy: from 0.3.0 before 0.9.0. T
CVE-2026-4203	A vulnerability was detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-3 remotely. The exploit is now public and may be used.
CVE-2026-24125	Tina is a headless content management system. Prior to 2.1.2, TinaCMS allows users to create, update, and delete content documents using relative file paths (rela
CVE-2026-4204	A flaw has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, D command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.
CVE-2026-4205	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS
CVE-2026-4206	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L
CVE-2026-4207	A vulnerability was determined in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS
CVE-2026-4209	A vulnerability was identified in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-3 leads to command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.
CVE-2026-4185	A vulnerability was found in GPAC up to 2.5-DEV-rev2167-gcc9d617c0-master. This vulnerability affects the function swf_def_bits_jpeg of the file src/scene_manage
CVE-2025-13913	A privileged Ignition user, intentionally or otherwise, imports an external file with a specially crafted payload, which executes embedded malicious code.
CVE-2026-4173	A flaw has been found in CodePhiliaX Chat2DB up to 0.3.7. This vulnerability affects the function exportTable/exportTableColumnComment/exportView/exportProce
CVE-2026-4171	A security vulnerability has been detected in CodeGenieApp serverless-express up to 4.17.1. Affected by this issue is some unknown functionality of the file examp
CVE-2026-3967	A flaw has been found in Alfresco Activiti up to 7.19/8.8.0. Affected by this issue is the function deserialize/createObjectInputStream of the file activiti-core/activiti-e
CVE-2026-3966	A vulnerability was detected in 648540858 wvp-GB28181-pro up to 2.7.4-20260107. Affected by this vulnerability is the function getDownloadFilePath of the file /s
CVE-2026-3965	A security vulnerability has been detected in whyour qinglong up to 2.20.1. Affected is an unknown function of the file back/loaders/express.ts of the component AI beforehand about the issues. He reacted very fast and highly professional.
CVE-2026-3961	A vulnerability was determined in zyddnys manga-image-translator up to beta-0.3. The affected element is the function to_pil_image of the file manga-image-trans
CVE-2026-3992	A weakness has been identified in CodeGenieApp serverless-express up to 4.17.1. This affects an unknown part of the file utils/dynamodb.ts of the component Use
CVE-2026-3958	A vulnerability has been found in Woahai321 ListSync up to 0.6.6. This issue affects the function requests.post of the file list-sync-main/api_server.py of the compo
CVE-2026-32128	FastGPT is an AI Agent building platform. In 4.14.7 and earlier, FastGPT's Python Sandbox (fastgpt-sandbox) includes guardrails intended to prevent file writes (stat
CVE-2026-3955	A security vulnerability has been detected in elecV2P up to 3.8.3. Affected by this issue is the function runJSFile of the file source-code/elecV2P-master/webser/wbj
CVE-2026-32451	Missing Authorization vulnerability in ThemeFusion Fusion Builder fusion-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue a
CVE-	

2026-32745	In JetBrains Datalore before 2026.1 session hijacking was possible due to missing secure attribute for cookie settings
CVE-2026-4013	A vulnerability was identified in SourceCodester Web-based Pharmacy Product Management System 1.0. This affects an unknown function of the file add_admin.ph
CVE-2025-25277	in OpenHarmony v5.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through using incompatible type. This vulnerability c
CVE-2026-30868	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.4, multiple OPNsense MVC API endpoints perform state-changing operations but are acces results in an authenticated Cross-Site Request Forgery vulnerability allowing unauthorized system state changes. This vulnerability is fixed in 26.1.4.
CVE-2026-20165	In Splunk Enterprise versions below 10.2.1, 10.0.4, 9.4.9, and 9.3.10, and Splunk Cloud Platform versions below 10.2.2510.7, 10.1.2507.17, 10.0.2503.12, and 9.3.
CVE-2026-20162	In Splunk Enterprise versions below 10.2.0, 10.0.3, 9.4.9, and 9.3.9, and Splunk Cloud Platform versions below 10.2.2510.4, 10.1.2507.15, 10.0.2503.11, and 9.3.2 vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The authenticated user should not be able to e
CVE-2026-4039	A vulnerability was determined in OpenClaw 2026.2.19-2. This vulnerability affects the function applySkillConfigenvOverrides of the component Skill Env Handler. E
CVE-2025-60012	Malicious configuration can lead to unauthorized file access in Apache Livy. This issue affects Apache Livy 0.7.0 and 0.8.0 when connecting to Apache Spark 3.1 or later, which fixes the issue.
CVE-2026-3968	A vulnerability has been found in AutohomeCorp frostmourne up to 1.0. This affects the function scriptEngine.eval of the file ExpressionRule.java of the component
CVE-2026-4230	A vulnerability has been found in vanna-ai vanna up to 2.0.2. Affected is the function update_sql of the file src/vanna/legacy/flask/__init__.py of the component End
CVE-2026-4241	A vulnerability was identified in itsourcecode College Management System 1.0. The impacted element is an unknown function of the file /admin/time-table.php. Suc
CVE-2026-4234	A security flaw has been discovered in SSCMS 7.4.0. This vulnerability affects unknown code of the file SitesAddController.Submit.cs of the component DDL Handle
CVE-2026-4308	A weakness has been identified in frdel/agent0ai agent-zero 0.9.7. This affects the function handle_pdf_document of the file python/helpers/document_query.py. Th
CVE-2026-4210	A security flaw has been discovered in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326 attacks.
CVE-2026-4228	A vulnerability was detected in LB-LINK BL-WR9000 2.4.9. This affects the function sub_458754 of the file /goform/set_wifi. The manipulation results in command in
CVE-2026-4215	A security flaw has been discovered in FlowCI flow-core-x up to 1.23.01. The impacted element is the function Save of the file core/src/main/java/com/flowci/core/co
CVE-2019-25484	WinMPG iPod Convert 3.0 contains a buffer overflow vulnerability in the Register dialog that allows local attackers to crash the application by supplying an oversize
CVE-2019-25485	R 3.4.4 on Windows x64 contains a buffer overflow vulnerability in the GUI Preferences language menu field that allows local attackers to bypass DEP and ASLR pro
CVE-2016-20029	ZKTeco ZKBioSecurity 3.0 contains a file path manipulation vulnerability that allows attackers to access arbitrary files by modifying file paths used to retrieve local
CVE-2019-25476	Outlook Password Recovery 2.10 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload. Att
CVE-2019-25475	SQL Server Password Changer 1.90 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload. A
CVE-2019-25474	Easy MP3 Downloader 4.7.8.8 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long unlock co

CVE-2019-25469	Folder Lock 7.7.9 contains a buffer overflow vulnerability in the serial number registration field that allows local attackers to crash the application by submitting an
CVE-2019-25463	SpotIE Internet Explorer Password Recovery 2.9.5 contains a denial of service vulnerability in the registration key input field that allows local attackers to crash the
CVE-2019-25477	RAR Password Recovery 1.80 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload in the re
CVE-2026-29066	Tina is a headless content management system. Prior to 2.1.8, the TinaCMS CLI dev server configures Vite with server.fs.strict: false, which disables Vite's built-in f
CVE-2026-3904	Calling NSS-backed functions that support caching via nscd may call the nscd client side code and in the GNU C Library version 2.36 under high load on x86_64 sys memcmp was introduced for x86_64 which could crash when invoked with such undefined behaviour, turning this into a potential crash of the nscd client and the a crash in the nscd client.
CVE-2025-58427	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2026-3884	Versions of the package spin.js before 3.0.0 are vulnerable to Cross-site Scripting (XSS) via the spin() function that allows a creation of more than 1 alert for each 't
CVE-2026-3824	IFTOP developed by WellChoose has an Open redirect vulnerability, allowing authenticated remote attackers to craft a URL that tricks users into visiting malicious v
CVE-2026-3825	IFTOP developed by WellChoose has a Reflected Cross-site Scripting vulnerability, allowing authenticated remote attackers to execute arbitrary JavaScript codes in
CVE-2016-20027	ZKTeco ZKBioSecurity 3.0 contains multiple reflected cross-site scripting vulnerabilities that allow attackers to execute arbitrary HTML and script code by injecting
CVE-2015-20116	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize CSV file uploads, allowing attackers to inject malicious scripts through filename parameters in multi
CVE-2015-20114	Next Click Ventures RealtyScript 4.0.2 contains a cross-site scripting vulnerability that allows attackers to execute arbitrary HTML and script code by injecting malic
CVE-2025-64735	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2026-1652	A potential buffer overflow vulnerability was reported in the Lenovo Virtual Bus driver used in Smart Connect that could allow a local authenticated user to corrupt
CVE-2025-47873	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-65119	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-66000	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-66042	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-66503	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-66617	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-66633	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2026-20726	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-	

2026-22882	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-64776	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2016-20036	Wowza Streaming Engine 4.5.0 contains multiple reflected cross-site scripting vulnerabilities in the enginemanager interface where input passed through various p
CVE-2025-57543	Cross Site scripting vulnerability (XSS) in NetBox 4.3.5 "comment" field on object forms. An attacker can inject arbitrary HTML, which will be rendered in the web U
CVE-2026-31859	Craft is a content management system (CMS). The fix for CVE-2025-35939 in craftcms/cms introduced a strip_tags() call in src/web/User.php to sanitize return URLs
CVE-2026-3442	A flaw was found in GNU Binutils. This vulnerability, a heap-based buffer overflow, specifically an out-of-bounds read, exists in the bfd linker component. An attacke
CVE-2026-3441	A flaw was found in GNU Binutils. This heap-based buffer overflow vulnerability, specifically an out-of-bounds read in the bfd linker, allows an attacker to gain acces
CVE-2026-20116	A vulnerability in the web-based management interface of Cisco Finesse, Cisco Packaged Contact Center Enterprise (Packaged CCE), Cisco Unified Contact C exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script coo
CVE-2026-20117	A vulnerability in the web-based management interface of Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to c of the affected interface or access sensitive, browser-based information.
CVE-2025-61952	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-61979	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-62403	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-69245	Raytha CMS is vulnerable to Reflected XSS via returnUrl parameter in logon functionality. An attacker can craft a malicious URL which, when opened by the authen
CVE-2026-29520	Hereta ETH-IMC408M firmware version 1.0.15 and prior contain a reflected cross-site scripting vulnerability in the Network Diagnosis ping function that allows attac
CVE-2026-4179	Issues in stm32 USB device driver (drivers/usb/device/usb_dc_stm32.c) can lead to an infinite while loop.
CVE-2025-62500	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2025-12473	The RTMKit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'themebuilder' parameter in all versions up to, and including, 1.6.8 due to in
CVE-2026-2324	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and inc
CVE-2025-64733	An out-of-bounds read vulnerability exists in the EMF functionality of Canva Affinity. By using a specially crafted EMF file, an attacker could exploit this vulnerability
CVE-2026-30882	Chamilo LMS is a learning management system. Chamilo LMS version 1.11.34 and prior contains a Reflected Cross-Site Scripting (XSS) vulnerability in the session c 20 (the page limit). This issue has been patched in version 1.11.36.
CVE-2017-20219	Serviio PRO 1.8 DLNA Media Streaming Server contains a DOM-based cross-site scripting vulnerability that allows attackers to execute arbitrary HTML and script co
CVE-2025-69242	Raytha CMS is vulnerable to reflected XSS via the backToListUrl parameter. An attacker can craft a malicious URL which, when opened by authenticated victim, res
CVE-	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.4 and 8.6.30, an attacker can upload a

2026-31868	vulnerability that can be exploited to steal session tokens, redirect users, or perform actions on behalf of other users. Affected file extensions and content types inc
CVE-2026-22192	wpDiscuz before 7.6.47 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript by importing a crafted c
CVE-2026-22183	wpDiscuz before 7.6.47 contains a stored cross-site scripting vulnerability in the inline comment preview functionality that allows authenticated users to inject mali
CVE-2026-2987	The Simple Ajax Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'c' parameter in versions up to, and including, 20260217 due to insuf
CVE-2025-13702	IBM Sterling Partner Engagement Manager 6.2.3.0 through 6.2.3.5 and 6.2.4.0 through 6.2.4.2 is vulnerable to cross-site scripting. This vulnerability allows an auth
CVE-2026-31860	Unhead is a document head and template manager. Prior to 2.1.11, useHeadSafe() can be bypassed to inject arbitrary HTML attributes, including event handlers, in
CVE-2026-1867	The Guest posting / Frontend Posting / Front Editor WordPress plugin before 5.0.6 allows passing a URL parameter to regenerate a .json file based on demo data th
CVE-2026-32351	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in blubrry PowerPress Podcasting powerpress allows Stored XSS.T
CVE-2026-32235	Backstage is an open framework for building developer portals. Prior to 0.27.1, the experimental OIDC provider in @backstage/plugin-auth-backend is vulnerable to can exchange it for a valid access token. This requires victim interaction and that one of the experimental features is explicitly enabled, which is not the default. Th
CVE-2026-31875	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.7 and 8.6.33, when multi-factor authen protected accounts. An attacker who obtains a single recovery code can repeatedly authenticate as the affected user without the code ever being invalidated. This
CVE-2026-32360	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in richplugins Rich Showcase for Google Reviews widget-google-r
CVE-2026-32419	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fernando Briano List category posts list-category-posts allows
CVE-2026-2581	This is an uncontrolled resource consumption vulnerability (CWE-400) that can lead to Denial of Service (DoS). In vulnerable Undici versions, when interceptors.dec endpoints that may produce large or long-lived response bodies. PatchesThe issue has been patched by changing deduplication behavior to stream response chunk
CVE-2026-32462	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liton Arefin Master Addons for Elementor master-addons allow
CVE-2026-3099	A flaw was found in Libsoup. The server-side digest authentication implementation in the SoupAuthDomainDigest class does not properly track issued nonces or en
CVE-2025-52644	HCL AION is affected by a vulnerability where certain user actions are not adequately audited or logged. The absence of proper auditing mechanisms may reduce t
CVE-2026-2454	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to handle incorrectly reported array lengths which allows malicious user to caus
CVE-2025-14806	IBM Planning Analytics Local 2.1.0 through 2.1.17 could allow an attacker to trick the caching mechanism into storing and serving sensitive, user-specific responses
CVE-2026-31853	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-16 and 6.9.13-41, an overflow on 32-bit systems can
CVE-2026-4349	A vulnerability was determined in Duende IdentityServer 4. The affected element is an unknown function of the file /connect/authorize of the component Token Ren
CVE-2025-52638	HCL AION is affected by a vulnerability where generated containers may execute binaries with root-level privileges. Running containers with root privileges may inc
CVE-2026-31890	Inspektor Gadget is a set of tools and framework for data collection and system inspection on Kubernetes clusters and Linux hosts using eBPF. Prior to 0.50.1, in a s the ring-buffer for the gadgets is hard-coded to 256KB. When a gadget_reserve_buf fails because of insufficient space, the gadget silently cleans up without produc
CVE-2025-	in OpenHarmony v5.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can b

52458	
CVE-2026-22209	wpDiscuz before 7.6.47 contains a cross-site scripting vulnerability in the customCss field that allows administrators to inject malicious scripts by breaking out of st
CVE-2026-4270	Improper Protection of Alternate Path exists in the no-access and workdir feature of the AWS API MCP Server versions >= 0.2.14 and < 1.3.9 on all platforms may a
CVE-2019-25464	InputMapper 1.6.10 contains a buffer overflow vulnerability in the username field that allows local attackers to crash the application by entering an excessively lon
CVE-2026-21294	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a Server-Side Request Forgery (SSRF) vulne
CVE-2016-20031	ZKTeco ZKBioSecurity 3.0 contains a local authorization bypass vulnerability in visLogin.jsp that allows attackers to authenticate without valid credentials by spoofi
CVE-2026-21293	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a Server-Side Request Forgery (SSRF) vulne
CVE-2026-3563	Improper input validation in the apps and endpoints configuration in PowerShell Universal before 2026.1.4 allows an authenticated user with permissions to create
CVE-2026-1653	A potential divide by zero vulnerability was reported in the Lenovo Virtual Bus driver used in Smart Connect that could allow a local authenticated user to cause a V
CVE-2026-21991	A DTrace component, dtprobed, allows arbitrary file creation through crafted USDT provider names.
CVE-2026-1717	An input validation vulnerability was reported in the LenovoProductivitySystemAddin used in Lenovo Vantage and Lenovo Baiying that could allow a local authentic
CVE-2026-2640	During an internal security assessment, a potential vulnerability was discovered in Lenovo PC Manager that could allow a local authenticated user to terminate priv
CVE-2026-31961	Quill provides simple mac binary signing and notarization from any platform. Quill before version v0.7.1 contains an unbounded memory allocation vulnerability wh signing structures (SuperBlob, BlobIndex) and uses them to allocate memory buffers without validating that the values are reasonable or consistent with the actual process. Both the Quill CLI and Go library are affected when used to parse untrusted Mach-O files. This vulnerability is fixed in 0.7.1.
CVE-2025-41432	in OpenHarmony v5.1.0 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can b
CVE-2026-27257	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27250	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32104	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.3, the updateUserNotifications endpoint accepts a user ID fro
CVE-2026-27248	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27256	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-31879	Frappe is a full-stack web application framework. Prior to 14.100.2, 15.101.0, and 16.10.0, due to a lack of validation and improper permission checks, users could
CVE-2025-65734	An authenticated arbitrary file upload vulnerability in the Courses/Work Assignments module of gunet Open eClass v3.11, and fixed in v3.13, allows attackers to ex
CVE-2026-31876	Notesnook is a note-taking app focused on user privacy & ease of use. Prior to 3.3.9, a Stored Cross-Site Scripting (XSS) vulnerability existed in Notesnook's editor
CVE-2026-	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att

27247	
CVE-2026-27244	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32587	Missing Authorization vulnerability in Saad Iqbal WP EasyPay allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP EasyPay:
CVE-2026-29510	Hereta ETH-IMC408M firmware version 1.0.15 and prior contain a stored cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary Java
CVE-2026-32391	Missing Authorization vulnerability in linethemes SmartFix smartfix allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SmartF
CVE-2026-32390	Missing Authorization vulnerability in linethemes Nanosoft nanosoft allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Nanos
CVE-2026-32388	Missing Authorization vulnerability in linethemes GLB glb allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GLB: from n/a th
CVE-2026-32420	Cross-Site Request Forgery (CSRF) vulnerability in Ruben Garcia GamiPress gamipress allows Cross Site Request Forgery.This issue affects GamiPress: from n/a thr
CVE-2026-32386	Missing Authorization vulnerability in EnvoThemes Envo Extra envo-extra allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects E
CVE-2026-32385	Missing Authorization vulnerability in Metagauss RegistrationMagic custom-registration-form-builder-with-submission-manager allows Exploiting Incorrectly Configu
CVE-2026-32423	Missing Authorization vulnerability in Bowo Admin and Site Enhancements (ASE) admin-site-enhancements allows Exploiting Incorrectly Configured Access Control
CVE-2026-27249	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27266	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32416	Missing Authorization vulnerability in bPlugins PDF Poster pdf-poster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PDF P
CVE-2026-2879	The GetGenie plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.2. This is due to missing validation on t arbitrary posts owned by any user — including Administrators — effectively destroying the original content by changing its `post_type` to `getgenie_chat` and reas
CVE-2026-29513	Hereta ETH-IMC408M firmware version 1.0.15 and prior contain a stored cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary Java
CVE-2026-27242	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-4324	A flaw was found in the Katello plugin for Red Hat Satellite. This vulnerability, caused by improper sanitization of user-provided input, allows a remote attacker to in
CVE-2026-32118	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, stored cross-site scripting (XSS) in the
CVE-2026-27255	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32417	Missing Authorization vulnerability in wppochipp Pochipp pochipp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Pochipp
CVE-2026-21292	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab
CVE-2026-	Plunk is an open-source email platform built on top of AWS SES. Prior to 0.7.1, Plunk's image upload endpoint accepted SVG files, which browsers treat as active do

32095	
CVE-2026-32412	Server-Side Request Forgery (SSRF) vulnerability in Gift Up! Gift Up Gift Cards for WordPress and WooCommerce gift-up allows Server Side Request Forgery.This iss
CVE-2026-32612	Statamic is a Laravel and Git powered content management system (CMS). Prior to 6.6.2, stored XSS in the control panel color mode preference allows authenticat
CVE-2026-27254	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27253	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27252	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2025-69693	Out-of-bounds read in FFmpeg 8.0 and 8.0.1 RV60 video decoder (libavcodec/rv60dec.c). The quantization parameter (qp) validation at line 2267 only checks the lo in commit 61cbcaf93f added validation only for intra frames. This vulnerability affects the released versions 8.0 (released 2025-08-22) and 8.0.1 (released 2025-11
CVE-2026-32124	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, the dynamic code picker AJAX endpoi
CVE-2026-27251	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27265	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27262	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-32125	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, track/item names from the Track Anyt
CVE-2026-32328	Cross-Site Request Forgery (CSRF) vulnerability in shufflehound Lemmony lemmony allows Cross Site Request Forgery.This issue affects Lemmony: from n/a throug
CVE-2026-27223	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-32139	Dataease is an open source data visualization analysis tool. In DataEase 2.10.19 and earlier, the static resource upload interface allows SVG uploads. However, bac 2.10.20.
CVE-2025-69236	Raytha CMS is vulnerable to Stored XSS via FieldValues[1].Value parameter in post editing functionality. Authenticated attacker with permissions to edit posts can
CVE-2026-32709	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, An unauthenticated path traversal vulnerability in the PX4 Autopilot MAVLink FTP implement function unconditionally returns true, providing no protection. A TOCTOU race condition in the write validation on NuttX further allows bypassing the only existing g
CVE-2026-27232	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27239	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-27231	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2025-69237	Raytha CMS is vulnerable to Stored XSS via FieldValues[0].Value parameter in page creation functionality. Authenticated attacker with permissions to create conte
CVE-2026-27234	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-0835	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1, and 6.2.2.0 are vulnerabl

CVE-2026-27235	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27240	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27230	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32840	Edimax GS-5008PL firmware version 1.00.54 and prior contain a stored cross-site scripting vulnerability in the system_name_set.cgi script that allows attackers to i
CVE-2026-20166	In Splunk Enterprise versions below 10.2.1 and 10.0.4, and Splunk Cloud Platform versions below 10.2.2510.5, 10.1.2507.16, and 10.0.2503.12, a low-privileged us
CVE-2025-69241	Raytha CMS is vulnerable to Stored XSS via FirstName and LastName parameters in profile editing functionality. Authenticated attacker can inject arbitrary HTML a
CVE-2026-27241	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27229	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2025-14504	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1, and 6.2.2.0 is vulnerable
CVE-2026-27228	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-27226	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-27237	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-32373	Missing Authorization vulnerability in Cozy Vision SMS Alert Order Notifications sms-alert allows Exploiting Incorrectly Configured Access Control Security Levels.Thi
CVE-2026-27225	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-2917	The Happy Addons for Elementor plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.21.0 via the `ha_dupl Contributor-level access and above, to clone any published post, page, or custom post type by obtaining a valid clone nonce from their own posts and changing the
CVE-2026-27236	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2023-40693	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, and 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1 are vulnerable to cros
CVE-2026-27224	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to injec
CVE-2026-27233	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged att
CVE-2026-31959	Quill provides simple mac binary signing and notarization from any platform. Quill before version v0.7.1 contains a Server-Side Request Forgery (SSRF) vulnerabilit violations are at risk. When retrieving submission logs, Quill fetches a URL provided in the API response without validating that the scheme is https or that the host notarization submission logs. This vulnerability is fixed in 0.7.1.
CVE-2026-31960	Quill provides simple mac binary signing and notarization from any platform. Quill before version v0.7.1 has unbounded reads of HTTP response bodies during the A HTTP responses during notarization, Quill reads the entire response body into memory without any size limit. An attacker who can control or modify the response c
CVE-2026-1068	An improper certificate validation vulnerability was reported in the Lenovo Filez application that could allow a user capable of intercepting network traffic to obtain

CVE-2025-69727	An Incorrect Access Control vulnerability exists in INDEX-EDUCATION PRONOTE prior to 2025.2.8. The affected components (index.js and composeUrlImgPhotoIndiv
CVE-2026-21286	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2026-32543	Missing Authorization vulnerability in CyberChimps Responsive Blocks responsive-block-editor-addons allows Exploiting Incorrectly Configured Access Control Secu
CVE-2026-32486	Missing Authorization vulnerability in wptravelengine Travel Booking travel-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issu
CVE-2026-2456	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 Mattermost fails to limit the size of responses from integration action endpoints, wh
CVE-2026-2233	The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to unauthorized modifi
CVE-2026-4015	A weakness has been identified in GPAC 26.03-DEV. Affected is the function txtin_process_texml of the file src/filters/load_text.c of the component TeXML File Parse
CVE-2026-32461	Missing Authorization vulnerability in Really Simple Plugins Really Simple SSL really-simple-ssl allows Exploiting Incorrectly Configured Access Control Security Leve
CVE-2026-30876	Chamilo LMS is a learning management system. Prior to version 1.11.36, Chamilo is vulnerable to user enumeration with valid/invalid username. This issue has bee
CVE-2026-32487	Missing Authorization vulnerability in raratheme Lawyer Landing Page lawyer-landing-page allows Exploiting Incorrectly Configured Access Control Security Levels.T
CVE-2013-20005	Qool CMS 2.0 RC2 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions by tricking logged-in users into visiting
CVE-2025-69243	Raytha CMS is vulnerable to User Enumeration in password reset functionality. Difference in messages could allow an attacker to determine if the login is valid or n
CVE-2026-22201	wpDiscuz before 7.6.47 contains an IP spoofing vulnerability in the getIP() function that allows attackers to bypass IP-based rate limiting and ban enforcement by tr
CVE-2026-32583	Missing Authorization vulnerability in Webnus Inc. Modern Events Calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2016-20035	Wowza Streaming Engine 4.5.0 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions by crafting malicious web
CVE-2026-4216	A weakness has been identified in i-SENS SmartLog App up to 2.6.8 on Android. This affects an unknown function of the component air.SmartLog.android. This mar application. This function is intended for configuration purposes related to device integration and testing. (...) [I]n a future application update, we plan to review me
CVE-2025-13723	IBM Sterling Partner Engagement Manager 6.2.3.0 through 6.2.3.5 and 6.2.4.0 through 6.2.4.2 could allow an attacker to obtain sensitive user information using an
CVE-2026-3783	When an OAuth2 bearer token is used for an HTTP(S) transfer, and that transfer performs a redirect to a second URL, curl could leak that token to the second hostn
CVE-2025-13726	IBM Sterling Partner Engagement Manager 6.2.3.0 through 6.2.3.5 and 6.2.4.0 through 6.2.4.2 could allow a remote attacker to obtain sensitive information when c
CVE-2026-31888	Shopware is an open commerce platform. Prior to 6.7.8.1 and 6.6.10.15, the Store API login endpoint (POST /store-api/account/login) returns different error codes d Store API does not — indicating an inconsistent defense. This vulnerability is fixed in 6.7.8.1 and 6.6.10.15.
CVE-2026-4199	A vulnerability was identified in bazinga012 mcp_code_executor up to 0.3.0. Affected by this issue is the function installDependencies of the file src/index.ts. Such
CVE-2026-4198	A vulnerability was determined in hypermodel-labs mcp-server-auto-commit 1.0.0. Affected by this vulnerability is the function getGitChanges of the file index.ts. T

CVE-2015-20117	Next Click Ventures RealtyScript 4.0.2 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to create unauthorized user accoun
CVE-2025-13212	IBM Aspera Console 3.3.0 through 3.4.8 could allow an authenticated user to cause a denial of service in the email service due to improper control of interaction fre
CVE-2026-29774	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, a client-side heap buffer overflow occurs in the FreeRDP client's AVC420/AVC444 can reach far beyond the allocated surface buffer. A malicious server sends a WIRE_TO_SURFACE_PDU_1 with AVC420 codec containing a regionRects entry where
CVE-2026-21310	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Improper Input Validation vulnerability th
CVE-2025-13460	IBM Aspera Console 3.3.0 through 3.4.8 could allow an attacker to enumerate usernames due to an observable response discrepancy.
CVE-2026-29775	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, a client-side heap out-of-bounds read/write occurs in FreeRDP's bitmap cache su
CVE-2015-20113	Next Click Ventures RealtyScript 4.0.2 contains cross-site request forgery and persistent cross-site scripting vulnerabilities that allow attackers to perform administ
CVE-2026-4187	A vulnerability was identified in Tiandy Easy7 Integrated Management Platform 7.17.0. Impacted is an unknown function of the file /WebService/UpdateLocalDevInf
CVE-2026-32724	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc1, a heap-use-after-free is detected in the MavlinkShell::available() function. The issue is cause
CVE-2026-32630	file-type detects the file type of a file, stream, or data. From 20.0.0 to 21.3.1, a crafted ZIP file can trigger excessive memory growth during type detection in file-ty
CVE-2026-4016	A security vulnerability has been detected in GPAC 26.03-DEV. Affected by this vulnerability is the function svgin_process of the file src/filters/load_svg.c of the com
CVE-2026-22199	wpDiscuz before 7.6.47 contains a vote manipulation vulnerability that allows attackers to manipulate comment votes by obtaining fresh nonces and bypassing rat
CVE-2026-4240	A vulnerability was determined in Open5GS up to 2.7.6. The affected element is the function smf_gx_cca_cb/smf_gy_cca_cb/smf_s6b_aaa_cb/smf_s6b_sta_cb of the
CVE-2026-31901	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.34 and 9.6.0-alpha.8, the email verification en with email verification enabled (verifyUserEmails: true). This vulnerability is fixed in 8.6.34 and 9.6.0-alpha.8.
CVE-2026-21282	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Improper Input Validation vulnerability th
CVE-2026-3856	IBM Db2 Recovery Expert for Linux, UNIX and Windows 5.5 IF 2 could allow an attacker to modify or corrupt data due to an insecure mechanism used for verifying t
CVE-2026-32457	Missing Authorization vulnerability in Wombat Plugins Advanced Product Fields (Product Addons) for WooCommerce advanced-product-fields-for-woocommerce allo
CVE-2026-32377	Missing Authorization vulnerability in raratheme Pranayama Yoga pranayama-yoga allows Exploiting Incorrectly Configured Access Control Security Levels.This issu
CVE-2026-32230	Uptime Kuma is an open source, self-hosted monitoring tool. From 2.0.0 to 2.1.3 , the GET /api/badge/:id/ping/:duration? endpoint in server/routers/api-router.js do
CVE-2026-32350	Missing Authorization vulnerability in wpradiant Chocolate House chocolate-house allows Exploiting Incorrectly Configured Access Control Security Levels.This issue
CVE-2026-32354	Insertion of Sensitive Information Into Sent Data vulnerability in magepeopleteam WpEvently mage-eventpress allows Retrieve Embedded Sensitive Data.This issue
CVE-2026-3964	A weakness has been identified in OpenAkita up to 1.24.3. This impacts the function run of the file src/openakita/tools/shell.py of the component Chat API Endpoint
CVE-	

2026-32100	Shopware is an open commerce platform. /api/_info/config route exposes information about active security fixes. This vulnerability is fixed in 2.0.16, 3.0.12, and 4.(
CVE-2026-31988	yauzl (aka Yet Another Unzip Library) version 3.2.0 for Node.js contains an off-by-one error in the NTFS extended timestamp extra field parser within the getLastMo entry.getLastModDate() on parsed entries. Fixed in version 3.2.1.
CVE-2026-3959	A vulnerability was found in 0xKoda WireMCP up to 7f45f8b2b4adeb76be8c6227eefb38533fdd6b1e. Impacted is the function server.tool of the file index.js of the c but has not responded yet.
CVE-2026-32362	Missing Authorization vulnerability in activity-log.com WP Sessions Time Monitoring Full Automatic activitytime allows Exploiting Incorrectly Configured Access Cont
CVE-2026-32363	Missing Authorization vulnerability in Funlus Oy WPLifeCycle free-php-version-info allows Exploiting Incorrectly Configured Access Control Security Levels.This issue
CVE-2026-2888	The Formidable Forms plugin for WordPress is vulnerable to an authorization bypass through user-controlled key in all versions up to, and including, 6.28. This is du authorization. This makes it possible for unauthenticated attackers to manipulate PaymentIntent amounts before payment completion on forms using dynamic pric
CVE-2026-3940	Insufficient policy enforcement in DevTools in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to bypass navigation restrictions via a crafted HTM
CVE-2026-3939	Insufficient policy enforcement in PDF in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to bypass navigation restrictions via a crafted PDF file. (
CVE-2026-32370	Missing Authorization vulnerability in ratheme Influencer influencer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Influ
CVE-2026-32371	Missing Authorization vulnerability in ratheme Elegant Pink elegant-pink allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2026-32372	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in RadiusTheme ShopBuilder – Elementor WooCommerce Builder Addons
CVE-2026-32374	Missing Authorization vulnerability in ratheme The Minimal the-minimal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2026-32375	Missing Authorization vulnerability in ratheme Travel Diaries travel-diaries allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec
CVE-2026-32348	Missing Authorization vulnerability in MadrasThemes MAS Videos masvideos allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec
CVE-2026-32347	Missing Authorization vulnerability in ratheme Restaurant and Cafe restaurant-and-cafe allows Exploiting Incorrectly Configured Access Control Security Levels.Th
CVE-2026-32346	Missing Authorization vulnerability in ratheme Travel Agency travel-agency allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affe
CVE-2026-32335	Missing Authorization vulnerability in ratheme The Conference the-conference allows Exploiting Incorrectly Configured Access Control Security Levels.This issue a
CVE-2026-3979	A flaw has been found in quickjs-ng quickjs up to 0.12.1. This affects the function js_iterator_concat_return of the file quickjs.c. This manipulation causes use after f
CVE-2026-31915	Missing Authorization vulnerability in UX-themes Flatsome flatsome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flatso
CVE-2026-31916	Missing Authorization vulnerability in Iulia Cazan Latest Post Shortcode latest-post-shortcode allows Exploiting Incorrectly Configured Access Control Security Level
CVE-2026-32322	soroban-sdk is a Rust SDK for Soroban contracts. Prior to 22.0.11, 23.5.3, and 25.3.0, The Fr (scalar field) types for BN254 and BLS12-381 in soroban-sdk compared that rely on Fr equality checks for security-critical logic could produce incorrect results. The impact depends on how the affected contract uses Fr equality comparis
CVE-2026-32329	Missing Authorization vulnerability in Ays Pro Advanced Related Posts advanced-related-posts allows Exploiting Incorrectly Configured Access Control Security Leve
CVE-	

2026-32332	Missing Authorization vulnerability in Ays Pro Easy Form easy-form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy F
CVE-2026-32334	Missing Authorization vulnerability in raratheme JobScout jobscout allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JobScou
CVE-2026-32336	Missing Authorization vulnerability in raratheme Rara Business rara-business allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affe
CVE-2026-32345	Missing Authorization vulnerability in raratheme Perfect Portfolio perfect-portfolio allows Exploiting Incorrectly Configured Access Control Security Levels.This issue
CVE-2026-32337	Missing Authorization vulnerability in raratheme Preschool and Kindergarten preschool-and-kindergarten allows Exploiting Incorrectly Configured Access Control Se
CVE-2026-32338	Missing Authorization vulnerability in raratheme Construction Landing Page construction-landing-page allows Exploiting Incorrectly Configured Access Control Secu
CVE-2026-32339	Missing Authorization vulnerability in raratheme Bakes And Cakes bakes-and-cakes allows Exploiting Incorrectly Configured Access Control Security Levels.This issu
CVE-2026-32340	Missing Authorization vulnerability in raratheme Business One Page business-one-page allows Exploiting Incorrectly Configured Access Control Security Levels.This
CVE-2026-32341	Missing Authorization vulnerability in raratheme Benevolent benevolent allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects B
CVE-2026-25771	Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 4.3.0 and prior to version 4.14.3, a Denial of Serv This forces the single-threaded event loop to pause for file read operations repeatedly, starving the application of CPU resources and potentially preventing it from
CVE-2026-32142	Shopware is an open commerce platform. /api/_info/config route exposes information about licenses. This vulnerability is fixed in 7.8.1 and 6.10.15.
CVE-2026-3994	A vulnerability was detected in rui314 mold up to 2.40.4. This issue affects the function mold::ObjectFilemold::X86_64::initialize_sections of the file src/input-files.c
CVE-2026-32376	Missing Authorization vulnerability in raratheme Kalon kalon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kalon: from n
CVE-2026-32378	Missing Authorization vulnerability in raratheme Book Landing Page book-landing-page allows Exploiting Incorrectly Configured Access Control Security Levels.This
CVE-2026-32379	Missing Authorization vulnerability in raratheme Rara Academic rara-academic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue af
CVE-2026-32425	Missing Authorization vulnerability in linknacional Payment Gateway Pix For GiveWP payment-gateway-pix-for-givewp allows Exploiting Incorrectly Configured Acce
CVE-2026-32427	Missing Authorization vulnerability in vowelweb VW Education Lite vw-education-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This iss
CVE-2026-32428	Missing Authorization vulnerability in Ays Pro Popup Like box ays-facebook-popup-likebox allows Exploiting Incorrectly Configured Access Control Security Levels.Th
CVE-2026-32111	ha-mcp is a Home Assistant MCP Server. Prior to 7.0.0, the ha-mcp OAuth consent form (beta feature) accepts a user-supplied ha_url and makes a server-side HTTP in 7.0.0.
CVE-2026-32432	Missing Authorization vulnerability in codepeople WP Time Slots Booking Form wp-time-slots-booking-form allows Exploiting Incorrectly Configured Access Control S
CVE-2026-32586	Missing Authorization vulnerability in Pluggabl Booster for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2026-32434	Missing Authorization vulnerability in vowelweb VW Fitness vw-fitness allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VW
CVE-	

2026-32435	Missing Authorization vulnerability in vowelweb VW Pet Shop vw-pet-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2026-32436	Missing Authorization vulnerability in vowelweb VW Photography vw-photography allows Exploiting Incorrectly Configured Access Control Security Levels.This issue
CVE-2026-32437	Missing Authorization vulnerability in vowelweb VW Portfolio vw-portfolio allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects \
CVE-2026-32438	Missing Authorization vulnerability in vowelweb VW School Education vw-school-education allows Exploiting Incorrectly Configured Access Control Security Levels.T
CVE-2026-32439	Missing Authorization vulnerability in WebGeniusLab BigHearts bighearts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects E
CVE-2026-32440	Missing Authorization vulnerability in Ex-Themes WP Food wp-food allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Foo
CVE-2026-32249	Vim is an open source, command line text editor. From 9.1.0011 to before 9.2.0137, Vim's NFA regex compiler, when encountering a collection containing a combi NULL check, causing a segmentation fault. This vulnerability is fixed in 9.2.0137.
CVE-2026-2373	The Royal Addons for Elementor – Addons and Templates Kit for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and inc
CVE-2026-32452	Missing Authorization vulnerability in ThemeFusion Fusion Builder fusion-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue a
CVE-2026-32453	Missing Authorization vulnerability in ThemeFusion Avada Core fusion-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects
CVE-2026-4271	A flaw was found in libsoup, a library for handling HTTP requests. This vulnerability, known as a Use-After-Free, occurs in the HTTP/2 server implementation. A remo
CVE-2026-1870	The Thim Kit for Elementor – Pre-built Templates & Widgets for Elementor plugin for WordPress is vulnerable to unauthorized access of data due to a missing valida
CVE-2026-32397	Missing Authorization vulnerability in YMC Filter & Grids ymc-smart-filter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects F
CVE-2026-32398	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Subrata Mal TeraWallet – For WooCommerce woo-wa
CVE-2026-32383	Missing Authorization vulnerability in ratheme Ridhi ridhi allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ridhi: from n/a
CVE-2026-32387	Missing Authorization vulnerability in Noor Alam Checkout for PayPal checkout-for-paypal allows Exploiting Incorrectly Configured Access Control Security Levels.Th
CVE-2026-3930	Unsafe navigation in Navigation in Google Chrome on iOS prior to 146.0.7680.71 allowed a remote attacker to bypass navigation restrictions via a crafted HTML pa
CVE-2026-32395	Missing Authorization vulnerability in Xpro Xpro Addons For Beaver Builder – Lite xpro-addons-beaver-builder-elementor allows Exploiting Incorrectly Config
CVE-2026-32396	Missing Authorization vulnerability in RadiusTheme Team tlp-team allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Team:
CVE-2026-32380	Missing Authorization vulnerability in ratheme Numinous numinous allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Num
CVE-2026-32402	Missing Authorization vulnerability in Ays Pro Image Slider by Ays ays-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec
CVE-2026-32381	Missing Authorization vulnerability in ratheme App Landing Page app-landing-page allows Exploiting Incorrectly Configured Access Control Security Levels.This is
CVE-2026-	Missing Authorization vulnerability in Studio99 Studio99 WP Monitor studio99-wp-monitor allows Exploiting Incorrectly Configured Access Control Security Levels.Th

32404	
CVE-2026-32405	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in xtemos WoodMart woodmart allows Retrieve Embedded Sensitive Dat
CVE-2026-32409	Missing Authorization vulnerability in WPMU DEV - Your All-in-One WordPress Platform Forminator forminator allows Exploiting Incorrectly Configured Access Contro
CVE-2026-32410	Missing Authorization vulnerability in WBW Plugins WBW Currency Switcher for WooCommerce woo-currency allows Exploiting Incorrectly Configured Access Contro
CVE-2026-32413	Missing Authorization vulnerability in Maciej Bis Permalink Manager Lite permalink-manager allows Exploiting Incorrectly Configured Access Control Security Levels
CVE-2026-32421	Missing Authorization vulnerability in Agile Logix Post Timeline post-timeline allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec
CVE-2026-32382	Missing Authorization vulnerability in ratheme Digital Download digital-download allows Exploiting Incorrectly Configured Access Control Security Levels.This issu
CVE-2026-32707	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, tattu_can contains an unbounded memcpy in its multi-frame assembly loop, allowing stack n
CVE-2026-0977	IBM CICS Transaction Gateway for Multiplatforms 9.3 and 10.1 could allow a user to transfer or view files due to improper access controls.
CVE-2026-3848	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.11 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-31798	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to v4.10.16-lts, JumpServer improperly validates certifica
CVE-2026-30853	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Prior to 9.5.0, a path traversal vulnerability in the RocketBook (
CVE-2026-31878	Frappe is a full-stack web application framework. Prior to 14.100.1, 15.100.0, and 16.6.0, a malicious user could send a crafted request to an endpoint which would
CVE-2026-0385	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability
CVE-2025-6969	in OpenHarmony v5.1.0 and prior versions allow a local attacker cause DOS through improper input.
CVE-2026-32415	Path Traversal: '.../...//' vulnerability in Bogdan Bendziukov Squeeze squeeze allows Path Traversal.This issue affects Squeeze: from n/a through <= 1.7.7.
CVE-2026-2376	A flaw was found in mirror-registry where an authenticated user can trick the system into accessing unintended internal or restricted systems by providing maliciou
CVE-2026-29516	Buffalo TeraStation NAS TS5400R firmware version 4.02-0.06 and prior contain an excessive file permissions vulnerability that allows authenticated attackers to re
CVE-2026-25772	Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 4.4.0 and prior to version 4.14.3, a stack-based b wraps around to a massive integer, effectively removing bounds checking for subsequent writes. This allows an attacker to corrupt the stack, leading to a Denial of
CVE-2026-32349	Server-Side Request Forgery (SSRF) vulnerability in Andy Fragen Embed PDF Viewer embed-pdf-viewer allows Server Side Request Forgery.This issue affects Embe
CVE-2026-22203	wpDiscuz before 7.6.47 contains an information disclosure vulnerability that allows administrators to inadvertently expose OAuth secrets by exporting plugin optio
CVE-2026-25790	Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 3.9.0 and prior to version 4.14.3, multiple stack-b `/src/analysisd/decoders/security_configuration_assessment.c`, within the `FillScanInfo` and `FillCheckEventInfo` functions. In multiple locations, a 128-byte buffer representation (a "1" followed by 150 zeros), which is larger than the 128-byte buffer, corrupting the stack. Version 4.14.3 patches the issue.
CVE-2026-	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerab

21291	
CVE-2026-31867	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 4.11.0 and 5.6.0, An Insecure Direct Object Reference (IDOR) vulnerability exists in Craft Comme shopping sessions and potential exposure of PII. This vulnerability is fixed in 4.11.0 and 5.6.0.
CVE-2026-31813	Supabase Auth is a JWT based API for managing users and issuing JWT tokens. Prior to 2.185.0, a vulnerability has been identified that allows an attacker to issue s existing OIDC identity (Apple or Azure) of the victim to an additional OIDC identity based on the ID token contents. The Auth server would then issue a valid user se
CVE-2025-52648	HCL AION is affected by a vulnerability where offering images are not digitally signed. Lack of image signing may allow the use of unverified or tampered images, p
CVE-2026-3957	A flaw has been found in xierongwkhd weimai-wetapp up to 5fe9e8225be4f73f2c5087f134aff657bdf1c6f2. This vulnerability affects the function getLikeMovieList o unavailable. The project was informed of the problem early through an issue report but has not responded yet.
CVE-2026-32290	The GL-iNet Comet (GL-RM1) KVM does not sufficiently verify the authenticity of uploaded firmware files. An attacker-in-the-middle or a compromised update serve
CVE-2026-32294	JetKVM prior to 0.5.4 does not verify the authenticity of downloaded firmware files. An attacker-in-the-middle or a compromised update server could modify the firr
CVE-2025-62320	HTML Injection can be carried out in Product when a web application does not properly check or clean user input before showing it on a webpage. Because of this, a
CVE-2026-3956	A vulnerability was detected in xierongwkhd weimai-wetapp up to 5fe9e8225be4f73f2c5087f134aff657bdf1c6f2. This affects the function getAdmins of the file sou project was informed of the problem early through an issue report but has not responded yet.
CVE-2026-32106	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.3, the REST API createUser endpoint uses string-based rank
CVE-2026-4284	A vulnerability was determined in taoofagi easegen-admin up to 8f87936ac774065b92fb20aab55b274a6ea76433. This issue affects the function downloadFile of th delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in
CVE-2026-32234	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.10 and 8.6.36, an attacker with access layer, this SQL injection bypasses Parse Server entirely and operates at the database level. This vulnerability only affects Parse Server deployments using PostgreS
CVE-2026-4253	A security flaw has been discovered in Tenda AC8 16.03.50.11. This affects the function route_set_user_policy_rule of the file /cgi-bin/UploadCfg of the component
CVE-2026-21359	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2025-52643	HCL AION is affected by a vulnerability where untrusted file parsing operations are not executed within a properly isolated sandbox environment. This may expose
CVE-2026-4238	A vulnerability has been found in itsourcecode College Management System 1.0. This issue affects some unknown processing of the file /admin/courses.php. The m
CVE-2026-4189	A weakness has been identified in phpipam up to 1.7.4. The impacted element is an unknown function of the file app/admin/sections/edit-result.php of the compon
CVE-2026-1527	ImpactWhen an application passes user-controlled input to the upgrade option of client.request(), an attacker can inject CRLF sequences (\r\n) to: * Inject arbitrary
CVE-2025-52637	HCL AION is affected by a vulnerability where certain offering configurations may permit execution of potentially harmful SQL queries. Improper validation or restri
CVE-2026-22210	wpDiscuz before 7.6.47 contains a cross-site scripting vulnerability that allows attackers to inject malicious code through unescaped attachment URLs in HTML outp
CVE-2026-32061	OpenClaw versions prior to 2026.2.17 contain a path traversal vulnerability in the $include directive resolution that allows reading arbitrary local files outside the c
CVE-2026-32237	Backstage is an open framework for building developer portals. Prior to 3.1.5, authenticated users with permission to execute scaffolder dry-runs can gain access t
CVE-2026-	Cross-Site Request Forgery (CSRF) vulnerability in Janis Elsts Admin Menu Editor admin-menu-editor allows Cross Site Request Forgery.This issue affects Admin Me

32456	
CVE-2026-3982	A vulnerability was determined in itsourcecode University Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_resul
CVE-2026-21297	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2026-21296	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2026-4063	The Social Icons Widget & Block by WPZOOM plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check in the add_me sharing configuration post with default sharing button settings, which causes social sharing buttons to be automatically injected into all post content on the fronter
CVE-2026-29521	Hereta ETH-IMC408M firmware version 1.0.15 and prior contain a cross-site request forgery vulnerability that allows attackers to modify device configuration by ex
CVE-2026-32839	Edimax GS-5008PL firmware version 1.00.54 and prior contain a cross-site request forgery vulnerability that allows remote attackers to perform unauthorized admi
CVE-2026-3226	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized email notification triggering due to missing capability checks on all 10 fu trigger arbitrary email notifications to admins, instructors, and users, enabling email flooding, social engineering, and impersonation of admin decisions regarding i
CVE-2026-31919	Missing Authorization vulnerability in Josh Kohlbach Advanced Coupons for WooCommerce Coupons advanced-coupons-for-woocommerce-free allows Exploiting Inc
CVE-2026-26304	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2 fail to verify run_create permission for empty playbookId, which allows team members to create unauthor
CVE-2026-1182	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.14 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-3951	A security flaw has been discovered in LockerProject Locker 0.0.0/0.0.1/0.1.0. Affected is the function authIsAwesome of the file source-code/Locker-master/Ops/re
CVE-2026-21285	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by an Incorrect Authorization vulnerability that
CVE-2026-32262	Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.5 and from version 5.0.0-RC1 to before version 5.9.11, the Asset permission on one volume to delete files in other folders/volumes that share the same filesystem root. This only affects local filesystems. This issue has been patch
CVE-2026-1663	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.4 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-1732	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.6 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2026-1629	Mattermost versions 10.11.x <= 10.11.10 Fail to invalidate cached permalink preview data when a user loses channel access which allows the user to continue vie
CVE-2026-3942	Incorrect security UI in PictureInPicture in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chron
CVE-2026-30961	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to 2.2.4, the chunked upload completion path for file requests do
CVE-2016-20028	ZKTeco ZKBioSecurity 3.0 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions by tricking logged-in users into
CVE-2026-3990	A security flaw has been discovered in CesiumGS CesiumJS up to 1.137.0. Affected by this issue is some unknown functionality of the file Apps/Sandcastle/standalo Apps/Sandcastle/standalone.html is part of the CesiumGS/cesium GitHub repository, but is demo code that is not part of the CesiumJS JavaScript library product."
CVE-2026-4233	A vulnerability was identified in ThingsGateway 12. This affects an unknown part of the file /api/file/download. The manipulation of the argument fileName leads to
CVE-2026-	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.6 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a

0602	
CVE-2026-1704	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all v appointment records belonging to other staff members and access sensitive customer personally identifiable information via the appointment ID parameter.
CVE-2026-22215	wpDiscuz before 7.6.47 contains a cross-site request forgery vulnerability in the getFollowsPage() function that allows attackers to trigger unauthorized actions wit
CVE-2025-14483	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_1, 6.2.1.0 through 6.2.1.1_1, and 6.2.2.0 could disclos
CVE-2017-20221	Telesquare SKT LTE Router SDT-CS3B1 version 1.2.0 contains a cross-site request forgery vulnerability that allows authenticated attackers to execute arbitrary sys
CVE-2026-3906	WordPress core is vulnerable to unauthorized access in versions 6.9 through 6.9.1. The Notes feature (block-level collaboration annotations) was introduced in Wor by other users, private posts, and posts in any status.
CVE-2026-3903	The Modular DS: Monitor, update, and backup multiple websites plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and includin
CVE-2026-1883	The Wicked Folders – Folder Organizer for Pages, Posts, and Custom Post Types plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versio
CVE-2025-15473	The Timetics WordPress plugin before 1.0.52 does not have authorization in a REST endpoint, allowing unauthenticated users to arbitrarily change a booking's payı
CVE-2026-2687	The Reading progressbar WordPress plugin before 1.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to
CVE-2026-4265	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to validate team-specific upload_file permissions which allows a guest user to p
CVE-2026-1948	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on
CVE-2026-21386	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to use consistent error responses when handling the /mute command which allo
CVE-2026-24692	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to properly enforce read permissions in search API endpoints which allows guest
CVE-2026-2455	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to canonicalize IPv4-mapped IPv6 addresses before reserved IP validation which
CVE-2026-3234	A flaw was found in mod_proxy_cluster. This vulnerability, a Carriage Return Line Feed (CRLF) injection in the decodeenc() function, allows a remote attacker to byp
CVE-2026-3993	A security vulnerability has been detected in itsourcecode Payroll Management System 1.0. This vulnerability affects unknown code of the file /manage_employee_
CVE-2026-30236	OpenProject is an open-source, web-based project management software. Prior to 17.2.0, when editing a project budget and planning the labor cost, it was not che calculate costs with the default rate of non-members. This vulnerability is fixed in 17.2.0.
CVE-2026-25780	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to bound memory allocation when processing DOC files which allows an authent
CVE-2026-32331	Missing Authorization vulnerability in Israpil Textmetrics webtexttool allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Textr
CVE-2026-3928	Insufficient policy enforcement in Extensions in Google Chrome prior to 146.0.7680.71 allowed an attacker who convinced a user to install a malicious extension to
CVE-2026-2578	Mattermost versions 11.3.x <= 11.3.0 fail to preserve the redacted state of burn-on-read posts during deletion which allows channel members to access unreveale
CVE-2026-	Incorrect security UI in PictureInPicture in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chron

3927	
CVE-2026-3925	Incorrect security UI in LookalikeChecks in Google Chrome on Android prior to 146.0.7680.71 allowed a remote attacker to perform UI spoofing via a crafted HTML
CVE-2026-32406	Missing Authorization vulnerability in WPClever WPC Product Bundles for WooCommerce woo-product-bundle allows Exploiting Incorrectly Configured Access Contr
CVE-2026-28506	Outline is a service that allows for collaborative documentation. Prior to 1.5.0, the events.list API endpoint, used for retrieving activity logs, contains a logic flaw in like the Document Title of Permanent Delete). Crucially, leaking valid Document IDs of deleted drafts removes the protection of UUID randomness, making High-se
CVE-2026-25783	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to properly validate User-Agent header tokens which allows an authenticated at
CVE-2026-32407	Missing Authorization vulnerability in WPClever WPC Smart Wishlist for WooCommerce woo-smart-wishlist allows Exploiting Incorrectly Configured Access Control S
CVE-2026-32408	Missing Authorization vulnerability in themefusecom Brizy brizy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Brizy: fron
CVE-2026-32447	Missing Authorization vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue
CVE-2025-69238	Raytha CMS is vulnerable to Cross-Site Request Forgery across multiple endpoints. Attacker can craft special website, which when visited by the authenticated vict
CVE-2026-32344	Cross-Site Request Forgery (CSRF) vulnerability in desertthemes Corpiva corpiva allows Cross Site Request Forgery.This issue affects Corpiva: from n/a through <=
CVE-2026-32343	Cross-Site Request Forgery (CSRF) vulnerability in Magazine3 Easy Table of Contents easy-table-of-contents allows Cross Site Request Forgery.This issue affects Ea
CVE-2026-32342	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker quiz-maker allows Cross Site Request Forgery.This issue affects Quiz Maker: from n/a through
CVE-2026-32330	Cross-Site Request Forgery (CSRF) vulnerability in 10Web Photo Gallery by 10Web photo-gallery allows Cross Site Request Forgery.This issue affects Photo Gallery
CVE-2026-32394	Missing Authorization vulnerability in PublishPress PublishPress Capabilities capability-manager-enhanced allows Exploiting Incorrectly Configured Access Control S
CVE-2026-32122	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.0.0.1, the Claim File Tracker feature exposes
CVE-2026-28563	Apache Airflow versions 3.1.0 through 3.1.7 /ui/dependencies endpoint returns the full DAG dependency graph without filtering by authorized DAG IDs. This allows
CVE-2026-2463	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to filter invite IDs based on user permissions, which allows regular users to bypa
CVE-2026-3938	Insufficient policy enforcement in Clipboard in Google Chrome prior to 146.0.7680.71 allowed a remote attacker who had compromised the renderer process to lea
CVE-2026-2461	Mattermost Plugins versions <=11.3 11.0.3 11.2.2 10.10.11.0 fail to implement authorisation checks on comment block modifications, which allows an authorised
CVE-2025-12555	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.1 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that, under certain condit
CVE-2026-32442	Missing Authorization vulnerability in E2Pdf e2pdf e2pdf allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects e2pdf: from n/a th
CVE-2026-2458	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to properly validate team membership when searching channels which allows a
CVE-2026-	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to sanitize client-supplied post metadata which allows an authenticated attacke

2457	
CVE-2026-4307	A security flaw has been discovered in frdel/agent0ai agent-zero 0.9.7-10. The impacted element is the function get_abs_path of the file python/helpers/files.py. Th
CVE-2026-3962	A vulnerability was identified in Jcharis Machine-Learning-Web-Apps up to a6996b634d98ccec4701ac8934016e8175b60eb5. The impacted element is the function affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.
CVE-2026-32713	PX4 autopilot is a flight control solution for drones. Prior to 1.17.0-rc2, A logic error in the PX4 Autopilot MAVLink FTP session validation uses incorrect boolean logic
CVE-2026-3941	Insufficient policy enforcement in DevTools in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to bypass navigation restrictions via a crafted HTM
CVE-2026-32446	Missing Authorization vulnerability in Syed Balkhi Contact Form by WPForms wpforms-lite allows Exploiting Incorrectly Configured Access Control Security Levels.Th
CVE-2026-26246	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10 fail to bound memory allocation when processing PSD image files which allows an a
CVE-2026-32719	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, The ImportedPlug
CVE-2026-3429	A flaw was identified in the Account REST API of Keycloak that allows a user authenticated at a lower security level to perform sensitive actions intended only for hi
CVE-2026-1230	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 1.0 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed ar
CVE-2026-30943	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to 2.2.4, An insufficient authorization check in the file replace API
CVE-2026-32777	libexpat before 2.7.5 allows an infinite loop while parsing DTD content.
CVE-2026-32776	libexpat before 2.7.5 allows a NULL pointer dereference with empty external parameter entity content.
CVE-2026-3634	A flaw was found in libsoup. An attacker controlling the value used to set the Content-Type header can inject a Carriage Return Line Feed (CRLF) sequence due to i
CVE-2026-3633	A flaw was found in libsoup. A remote attacker, by controlling the method parameter of the `soup_message_new()` function, could inject arbitrary headers and add
CVE-2026-3632	A flaw was found in libsoup, a library used by applications to send network requests. This vulnerability occurs because libsoup does not properly validate hostname SoupServer is not actually used in internet infrastructure.
CVE-2026-4222	A vulnerability was determined in SSCMS up to 7.4.0. This vulnerability affects the function PathUtils.RemoveParentPath of the file /api/admin/plugins/install/actions
CVE-2026-4044	A vulnerability was detected in projectsend up to r1945. This affects the function realpath of the file /import-orphans.php of the component Delete Handler. Perform
CVE-2026-26230	Mattermost versions 10.11.x <= 10.11.10 fail to properly validate permission requirements in the team member roles API endpoint which allows team administrato
CVE-2026-0849	Malformed ATAES132A responses with an oversized length field overflow a 52-byte stack buffer in the Zephyr crypto driver, allowing a compromised device or bus
CVE-2026-32715	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, The two generic s
CVE-2026-3963	A security flaw has been discovered in perfree go-fastdfs-web up to 1.3.7. This affects the function rememberMeManager of the file src/main/java/com/perfree/conf any way.
CVE-2025-	Mumble before 1.6.870 is prone to an out-of-bounds array access, which may result in denial of service (client crash).

71264	
CVE-2025-62328	HCL Nomad server on Domino did not configure the frame-ancestors directive in the Content-Security-Policy header by default which could allow an attacker to obt
CVE-2025-13718	IBM Sterling Partner Engagement Manager 6.2.3.0 through 6.2.3.5 and 6.2.4.0 through 6.2.4.2 could allow a remote attacker to obtain sensitive information in clea
CVE-2026-32109	Copyparty is a portable file server. Prior to 1.20.12, if an attacker has been given both read- and write-permissions to the server, they can upload a malicious file w preventative measures (strict SameSite cookies) which makes it harder to leverage this vulnerability in an attack; in order to gain control of the target's authentica
CVE-2026-4045	A flaw has been found in projectsend up to r1945. This impacts an unknown function of the file includes/Classes/Auth.php. Executing a manipulation of the argume
CVE-2026-22204	wpDiscuz before 7.6.47 contains an email header injection vulnerability that allows attackers to manipulate mail recipients by injecting malicious data into the com
CVE-2026-32293	The GL-iNet Comet (GL-RM1) KVM connects to a GL-iNet site during boot-up to provision client and CA certificates. The GL-RM1 does not verify certificates used for
CVE-2026-24509	Dell Alienware Command Center (AWCC), versions prior to 6.12.24.0, contain an Improper Access Control vulnerability. A low privileged attacker with local access c
CVE-2026-31863	Anytype Heart is the middleware library for Anytype. The challenge-based authentication for the local gRPC client API can be bypassed, allowing an attacker to gai
CVE-2026-3983	A security flaw has been discovered in Campcodes Division Regional Athletic Meet Game Result Matrix System 2.1. This affects an unknown part of the file save-ga
CVE-2026-3946	A vulnerability was detected in PHPEMS 11.0. The affected element is an unknown function of the file /index.php?ask=app-ask. Performing a manipulation of the ar
CVE-2026-4186	A vulnerability was determined in UEditor up to 1.4.3.2. This issue affects some unknown processing of the file php/controller.php?action=uploadimage of the comp
CVE-2026-3984	A weakness has been identified in Campcodes Division Regional Athletic Meet Game Result Matrix System 2.1. This vulnerability affects unknown code of the file sa
CVE-2026-4239	A vulnerability was found in Lagom WHMCS Template up to 2.3.7. Impacted is an unknown function of the component Datatables. The manipulation results in impr
CVE-2026-4166	A vulnerability was found in Wavlink WL-NU516U1 240425. The impacted element is the function sub_404F68 of the file /cgi-bin/login.cgi. The manipulation of the a
CVE-2025-12704	GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed an a
CVE-2026-4175	A vulnerability was determined in Aureus ERP up to 1.3.0-BETA2. The affected element is an unknown function of the file plugins/webkul/chatter/resources/views/fil component.
CVE-2026-32772	telnet in GNU inetutils through 2.7 allows servers to read arbitrary environment variables from clients via NEW_ENVIRON SEND USERVAR.
CVE-2025-26474	in OpenHarmony v5.0.3 and prior versions allow a local attacker cause information improper input. This vulnerability can be exploited only in restricted scenarios.
CVE-2026-4012	A vulnerability was determined in rxi fe up to ed4cda96bd582cbb08520964ba627efb40f3dd91. The impacted element is the function read_ of the file src/fe.c. This
CVE-2025-52642	HCL AION is affected by a vulnerability where internal filesystem paths may be exposed through application responses or system behaviour. Exposure of internal p
CVE-2026-0639	in OpenHarmony v6.0 and prior versions allow a local attacker case DOS through missing release of memory.
CVE-2026-	A vulnerability was identified in OpenClaw up to 2026.2.17. This issue affects the function tools.exec.safeBins of the component File Existence Handler. The manipu

4040	
CVE-2026-3950	A vulnerability was identified in strukturag libheif up to 1.21.2. This impacts the function Track::load of the file libheif/sequences/track.cc of the component stsz/stt
CVE-2026-4009	A vulnerability has been found in jarikomppa soloud up to 20200207. Impacted is the function drwav_read_pcm_frames_s16__msadpcm in the library src/audiosour responded yet.
CVE-2026-3949	A vulnerability was determined in strukturag libheif up to 1.21.2. This affects the function vvdec_push_data2 of the file libheif/plugins/decoder_vvdec.cc of the com
CVE-2026-4219	A flaw has been found in INDEX Conferences & Exhibitions Organization YWF BPOF APGCS App up to 1.0.2 on Android. Affected by this vulnerability is an unknown
CVE-2026-4010	A vulnerability was found in ThakeeNathees pocketlang up to cc73ca61b113d48ee130d837a7a8b145e41de5ce. The affected element is the function pkByteBuffer/ yet.
CVE-2025-70330	Easy Grade Pro 4.1.0.2 contains a file parsing logic flaw in the handling of proprietary .EGP gradebook files. By modifying specific fields at precise offsets within an
CVE-2026-4174	A vulnerability has been found in Radare2 5.9.9. This issue affects the function walk_exports_trie of the file libr/bin/format/mach0/mach0.c of the component Mach- affected component. The code maintainer states that, "[he] wont consider this bug a DoS".
CVE-2025-14811	IBM Sterling Partner Engagement Manager 6.2.3.0 through 6.2.3.5 and 6.2.4.0 through 6.2.4.2 could allow an attacker to obtain sensitive information from the que
CVE-2026-22545	Mattermost versions 10.11.x <= 10.11.10 fail to validate user's authentication method when processing account auth type switch which allows an authenticated at
CVE-2026-21295	Adobe Commerce versions 2.4.9-alpha3, 2.4.8-p3, 2.4.7-p8, 2.4.6-p13, 2.4.5-p15, 2.4.4-p16 and earlier are affected by a URL Redirection to Untrusted Site ('Open I
CVE-2026-29776	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, Integer Underflow in update_read_cache_bitmap_order Function of FreeRDP's Co
CVE-2026-3929	Side-channel information leakage in ResourceTiming in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to leak cross-origin data via a crafted HTM
CVE-2026-2366	A flaw was found in Keycloak. An authorization bypass vulnerability in the Keycloak Admin API allows any authenticated user, even those without administrative pri
CVE-2026-31974	OpenProject is an open-source, web-based project management software. Prior to 17.2.0, OpenProject SMTP test endpoint (POST /admin/settings/mail_notifications kind of SSRF issue which allows attackers to scan the internal network. This vulnerability is fixed in 17.2.0.
CVE-2026-32778	libexpat before 2.7.5 allows a NULL pointer dereference in the function setContext on retry after an earlier ouf-of-memory condition.
CVE-2026-0520	A potential vulnerability was reported in the Lenovo FileZ Android application that, under certain conditions, could allow a local authenticated user to retrieve some
CVE-2025-69239	Raytha CMS is vulnerable to Server-Side Request Forgery in the “Themes - Import from URL” feature. It allows an attacker with high privileges to provide the URL f
CVE-2025-13459	IBM Aspera Console 3.3.0 through 3.4.8 could allow a privileged user to cause a denial of service due to improper enforcement of behavioral workflow.
CVE-2026-32445	Missing Authorization vulnerability in Elementor Elementor Website Builder elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This i
CVE-2026-32717	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, in multi-user mod even though normal authenticated requests are rejected.
CVE-2026-4285	A vulnerability was identified in taoofagi easegen-admin up to 8f87936ac774065b92fb20aab55b274a6ea76433. Impacted is the function recognizeMarkdown of th affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-	A flaw was found in Keycloak. An authenticated user with the view-users role could exploit a vulnerability in the UserResource component. By accessing a specific a

3911	
CVE-2025-31966	HCL Sametime is vulnerable to broken server-side validation. While the application performs client-side input checks, these are not enforced by the web server. An
CVE-2026-4242	A security flaw has been discovered in BabyChakra Pregnancy & Parenting App up to 5.4.3.0 on Android. This affects an unknown function of the file file app/babyc contacted early about this disclosure but did not respond in any way.
CVE-2026-4217	A security vulnerability has been detected in XREAL Nebula App up to 3.2.1 on Android. This impacts an unknown function of the file in ai/nreal/nebula/flutterPlugin contacted early about this disclosure but did not respond in any way.
CVE-2026-24508	Dell Alienware Command Center (AWCC), versions prior to 6.12.24.0, contain an Improper Certificate Validation vulnerability. A low privileged attacker with local ac
CVE-2026-4251	A vulnerability was determined in CityData CityChat up to 0.12.6 on Android. Affected by this vulnerability is an unknown functionality of the file resources/assets/f any way.
CVE-2026-4243	A weakness has been identified in La Nacion App 10.2.25 on Android. This impacts an unknown function of the file source/app/lanacion/clublanacion/BuildConfig.jav this disclosure but did not respond in any way.
CVE-2026-4250	A vulnerability was found in Albert Sağlık Hizmetleri ve Ticaret Albert Health up to 1.7.3 on Android. Affected is an unknown function of the file resources/assets/se
CVE-2026-4218	A vulnerability was detected in myAEDES App up to 1.18.4 on Android. Affected is an unknown function of the file aedes/me/beta/utils/EngageBayUtils.java of the c
CVE-2026-4168	A vulnerability was identified in Tecnick TCExam 16.5.0. This impacts an unknown function of the file /admin/code/tce_edit_group.php of the component Group Han Therefore, it can be assumed that this issue got fixed in a later release.
CVE-2026-4169	A security flaw has been discovered in Tecnick TCExam up to 16.6.0. Affected is the function F_xml_export_users of the file admin/code/tce_xml_users.php of the co another security issue, he identified and fixed this flaw during analysis. He doubts the impact of this: "However, this is difficult to justify as security issue. It require
CVE-2026-4165	A vulnerability has been found in Worksuite HR, CRM and Project Management up to 5.5.25. The affected element is an unknown function of the file /account/orders
CVE-2026-4225	A security flaw has been discovered in CMS Made Simple up to 2.2.21. Impacted is an unknown function of the file admin/listusers.php of the component User Mana
CVE-2025-12697	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.5 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2 that could have allowed a
CVE-2025-52646	HCL AION is affected by a vulnerability where certain offering configurations may permit execution of potentially harmful SQL queries. Improper validation or restri
CVE-2026-4359	A compromised third party cloud server or man-in-the-middle attacker could send a malformed HTTP response and cause a crash in applications using the MongoD
CVE-2025-52645	HCL AION is affected by a vulnerability where model packaging and distribution mechanisms may not include sufficient authenticity verification. This may allow the
CVE-2025-52636	HCL AION is affected by a vulnerability related to the handling of upload size limits. Improper control or validation of upload sizes may allow excessive resource con
CVE-2025-52649	HCL AION is affected by a vulnerability where certain identifiers may be predictable in nature. Predictable identifiers may allow an attacker to infer or guess system
CVE-2026-31897	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, there is an out-of-bounds read in freerdp_bitmap_decompress_planar when SrcS
CVE-2026-31873	Unhead is a document head and template manager. Prior to 2.1.11, The link.href check in makeTagSafe (safe.ts) uses String.includes(), which is case-sensitive. Bro
CVE-2026-32236	Backstage is an open framework for building developer portals. Prior to 0.27.1, a Server-Side Request Forgery (SSRF) vulnerability exists in @backstage/plugin-auth explicitly enabled via an experimental flag that is off by default. Deployments that restrict allowedClientIdPatterns to specific trusted domains are not affected. Pat
CVE-2026-	Emlog is an open source website building system. In 2.6.6 and earlier, the delete_async action (asynchronous delete) lacks a call to LoginAuth::checkToken(), enab

31954	
CVE-2026-1471	Excessive caching of authentication context in Neo4j Enterprise edition versions prior to 2026.01.4 leads to authenticated users inheriting the context of the first u
CVE-2026-2921	GStreamer RIFF Palette Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected inst execute code in the context of the current process. Was ZDI-CAN-28854.
CVE-2026-32635	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-next.3, 21.2.4 mechanism, which when combined with a data binding to untrusted user-generated data can allow an attacker to inject a malicious script. This vulnerability is fixe
CVE-2026-2859	Improper permission enforcement in Checkmk versions 2.4.0 before 2.4.0p23, 2.3.0 before 2.3.0p43, and 2.2.0 (EOL) allows unauthenticated users to enumerate e
CVE-2026-2491	Socomec DIRIS A-40 HTTP API Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected install
CVE-2026-31975	Cloud CLI (aka Claude Code UI) is a desktop and mobile UI for Claude Code, Cursor CLI, Codex, and Gemini-CLI. Prior to 1.25.0, OS Command Injection via WebSock
CVE-2025-13406	NULL Pointer Dereference vulnerability in Softing Industrial Automation GmbH smartLink SW-HT (Webserver modules) allows HTTP DoS.This issue affects smartLink
CVE-2026-4208	The extension fails to properly reset the generated MFA code after successful authentication. This leads to a possible MFA bypass for future login attempts by provi
CVE-2026-27260	Rejected reason: This CVE ID was issued in error by its CVE Numbering Authority.
CVE-2026-2493	IceWarp collaboration Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affect
CVE-2026-2920	GStreamer ASF Demuxer Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code or this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28843.
CVE-2026-21570	This High severity RCE (Remote Code Execution) vulnerability was introduced in versions 9.6.0, 10.0.0, 10.1.0, 10.2.0, 11.0.0, 11.1.0, 12.0.0, and 12.1.0 of Bambo than or equal to 9.6.24 Bamboo Data Center 10.2: Upgrade to a release greater than or equal to 10.2.16 Bamboo Data Center 12.1: Upgrade to a release greater th
CVE-2026-2923	GStreamer DVB Subtitles Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affecte in the context of the current process. Was ZDI-CAN-28838.
CVE-2026-32702	Cleanuparr is a tool for automating the cleanup of unwanted or blocked files in Sonarr, Radarr, and supported download clients like qBittorrent. From 2.7.0 to 2.8.0 introduced that exposes validity to the actor. This vulnerability is fixed in 2.8.1.
CVE-2026-31814	Yamux is a stream multiplexer over reliable, ordered connections such as TCP/IP. From 0.13.0 to before 0.13.9, a specially crafted WindowUpdate can cause arithm
CVE-2026-2922	GStreamer RealMedia Demuxer Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on execute code in the context of the current process. Was ZDI-CAN-28845.
CVE-2026-1524	An edgecase in SSO implementation in Neo4j Enterprise edition versions prior to version 2026.02 can lead to unauthorised access under the following conditions: If intended (configured) authorization provider. When using multiple plugins for authentication and authorisation, prior to the fix the issue could lead to a plugin confi
CVE-2026-32314	Yamux is a stream multiplexer over reliable, ordered connections such as TCP/IP. Prior to 0.13.10, the Rust implementation of Yamux can panic when processing a machine. This is remotely reachable over a normal Yamux session and does not require authentication. This vulnerability is fixed in 0.13.10.
CVE-2025-71239	In the Linux kernel, the following vulnerability has been resolved: audit: add fchmodat2() to change attributes class fchmodat2(), introduced in version 6.6 is curren
CVE-2026-31386	OpenLiteSpeed and LSWS Enterprise provided by LiteSpeed Technologies contain an OS command injection vulnerability. An arbitrary OS command may be execut
CVE-2026-32640	SimpleEval is a library for adding evaluatable expressions into python projects. Prior to 1.0.5, objects (including modules) can leak dangerous modules through to c
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: audit: add missing syscalls to read class The "at" variant of getxattr() and listxattr() are missing f

23241	
CVE-2026-27259	Rejected reason: This CVE ID was issued in error by its CVE Numbering Authority.
CVE-2026-30914	SFTPGo is an open source, event-driven file transfer solution. In SFTPGo versions prior to 2.7.1, a path normalization discrepancy between the protocol handlers an
CVE-2026-31854	Cursor is a code editor built for programming with AI. Prior to 2.0 ,if a visited website contains maliciously crafted instructions, the model may attempt to follow the
CVE-2026-30707	An issue was discovered in SpeedExam Online Examination System (SaaS) after v.FEV2026. It allows Broken Access Control via the ReviewAnswerDetails ASP.NET
CVE-2026-32837	miniaudio version 0.11.25 and earlier contain a heap out-of-bounds read vulnerability in the WAV BEXT metadata parser that allows attackers to trigger memory ac
CVE-2026-20997	Improper verification of cryptographic signature in Smart Switch prior to version 3.7.69.15 allows remote attackers to potentially bypass authentication.
CVE-2026-20996	Use of a broken or risky cryptographic algorithm in Smart Switch prior to version 3.7.69.15 allows remote attackers to configure a downgraded scheme for authent
CVE-2026-20995	Exposure of sensitive functionality to an unauthorized actor in Smart Switch prior to version 3.7.69.15 allows remote attackers to set a specific configuration.
CVE-2026-20994	URL redirection in Samsung Account prior to version 15.5.01.1 allows remote attackers to potentially get access token.
CVE-2025-15037	An Incorrect Permission Assignment vulnerability exists in the ASUS Business System Control Interface driver. This vulnerability can be triggered by an unprivileged
CVE-2026-2809	Netskope was notified about a potential gap in its Endpoint DLP Module for Netskope Client on Windows systems. The successful exploitation of the gap can potent
CVE-2025-15038	An Out-of-Bounds Read vulnerability exists in the ASUS Business System Control Interface driver. This vulnerability can be triggered by an unprivileged local user s
CVE-2026-1878	An Insufficient Integrity Verification vulnerability in the ASUS ROG peripheral driver installation process allows privilege escalation to SYSTEM. The vulnerability is d
CVE-2026-20993	Improper export of android application components in Samsung Assistant prior to version 9.3.10.7 allows local attacker to access saved information.
CVE-2026-20992	Improper authorization in Settings prior to SMR Mar-2026 Release 1 allows local attacker to disable configuring the background data usage of application.
CVE-2026-20991	Improper privilege management in ThemeManager prior to SMR Mar-2026 Release 1 allows local privileged attackers to reuse trial contents.
CVE-2026-20990	Improper export of android application components in Secure Folder prior to SMR Mar-2026 Release 1 allows local attackers to launch arbitrary activity with Secure
CVE-2026-20989	Improper verification of cryptographic signature in Font Settings prior to SMR Mar-2026 Release 1 allows physical attackers to use custom font.
CVE-2026-20988	Improper verification of intent by broadcast receiver in Settings prior to SMR Mar-2026 Release 1 allows local attacker to launch arbitrary activity with Settings priv
CVE-2026-3841	A command injection vulnerability has been identified in the Telnet command-line interface (CLI) of TP-Link TL-MR6400 v5.3. This issue is caused by insufficient san
CVE-2026-20643	A cross-origin issue in the Navigation API was addressed with improved input validation. This issue is fixed in Background Security Improvements for iOS 26.3.1, iPa
CVE-2026-	dr_libs version 0.13.3 and earlier contain an uncontrolled memory allocation vulnerability in drflac__read_and_decode_metadata() that allows attackers to trigger e

32836	
CVE-2026-20998	Improper authentication in Smart Switch prior to version 3.7.69.15 allows remote attackers to bypass authentication.
CVE-2026-2326	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car
CVE-2025-15584	Netskope was notified about a potential gap in its Endpoint DLP Module for Netskope Client on Windows systems. The successful exploitation of the gap can potent
CVE-2026-32240	Cap'n Proto is a data interchange format and capability-based RPC system. Prior to 1.4.0, when using Transfer-Encoding: chunked, if a chunk's size parsed to a valu
CVE-2026-32239	Cap'n Proto is a data interchange format and capability-based RPC system. Prior to 1.4.0, a negative Content-Length value was converted to unsigned, treating it a
CVE-2026-28256	A Use of Hard-coded, Security-relevant Constants vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive in
CVE-2026-3497	Vulnerability in the OpenSSH GSSAPI delta included in various Linux distributions. This vulnerability affects the GSSAPI patches added by various Linux distributions initialized to NULL the code later accesses those uninitialized variables, accessing random memory, which could lead to undefined behavior. The recommended wo
CVE-2026-0230	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on macOS allows a local administrator to disable the agent. This issue could be
CVE-2026-0231	An information disclosure vulnerability in Palo Alto Networks Cortex XDR® Broker VM allows an authenticated user to obtain and modify sensitive information by tr
CVE-2026-32232	ZeptoClaw is a personal AI assistant. Prior to 0.7.6, there is a Dangling Symlink Component Bypass, TOCTOU Between Validation and Use, and Hardlink Alias Bypas
CVE-2026-30915	SFTPGo is an open source, event-driven file transfer solution. SFTPGo versions before v2.7.1 contain an input validation issue in the handling of dynamic group patl This issue is fixed in version v2.7.1
CVE-2026-32129	soroban-poseidon provides Poseidon and Poseidon2 cryptographic hash functions for Soroban smart contracts. Poseidon V1 (PoseidonSponge) accepts variable-len poseidon_hash where the number of inputs is less than T - 1 (e.g., hashing 1 input with T=3). Poseidon2 (Poseidon2Sponge) is not affected.
CVE-2026-25083	GROWI OpenAI thread/message API endpoints do not perform authorization. Affected are v7.4.5 and earlier versions. A logged-in user who knows a shared AI assist
CVE-2026-21005	Path traversal in Smart Switch prior to version 3.7.69.15 allows adjacent attackers to overwrite arbitrary files with Smart Switch privilege.
CVE-2026-21004	Improper authentication in Smart Switch prior to version 3.7.69.15 allows adjacent attackers to trigger a denial of service.
CVE-2026-21002	Improper verification of cryptographic signature in Galaxy Store prior to version 4.6.03.8 allows local attacker to install arbitrary application.
CVE-2026-21001	Path traversal in Galaxy Store prior to version 4.6.03.8 allows local attacker to create file with Galaxy Store privilege.
CVE-2026-21000	Improper access control in Galaxy Store prior to version 4.6.03.8 allows local attacker to create file with Galaxy Store privilege.
CVE-2026-20999	Authentication bypass by replay in Smart Switch prior to version 3.7.69.15 allows remote attackers to trigger privileged functions.
CVE-2026-3207	Configuration issue in Java Management Extensions (JMX) in TIBCO BPM Enterprise version 4.x allows unauthorised access.
CVE-2026-4202	The extension fails to verify, if an authenticated user has permissions to access to redirects resulting in exposure of redirect records when editing a page.
CVE-2026-	Non-relational SQL injection vulnerability (NoSQLi) in the Wakyma web application, specifically in the endpoint 'vets.wakyma.com/centro/equipo/empleado'. This vu

3021	
CVE-2026-1323	The extension fails to properly define allowed classes used when deserializing transport failure metadata. An attacker may exploit this to execute untrusted serializ
CVE-2026-24097	Improper permission enforcement in Checkmk versions 2.4.0 before 2.4.0p23, 2.3.0 before 2.3.0p43, and 2.2.0 (EOL) allows authenticated users to enumerate exis
CVE-2025-13337	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-12455	Observable response discrepancy vulnerability in OpenText™ Vertica allows Password Brute Forcing. The vulnerability could lead to Password Brute Forcing in Ver
CVE-2025-12454	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OpenText™ Vertica allows Reflected XSS. The vulnerability coul
CVE-2025-12453	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OpenText™ Vertica allows Reflected XSS. The vulnerability coul
CVE-2026-3561	Philips Hue Bridge hk_hap characteristics Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28479.
CVE-2026-3560	Philips Hue Bridge HomeKit hk_hap_pair_storage_put Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28469.
CVE-2026-27842	Authentication bypass issue exists in MR-GM5L-S1 and MR-GM5A-L1, which may allow an attacker to bypass authentication and change the device configuration.
CVE-2026-24448	Use of hard-coded credentials issue exists in MR-GM5L-S1 and MR-GM5A-L1, which may allow an attacker to obtain administrative access.
CVE-2026-3559	Philips Hue Bridge HomeKit Accessory Protocol Static Nonce Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass aut the system. Was ZDI-CAN-28451.
CVE-2026-28252	A Use of a Broken or Risky Cryptographic Algorithm vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to bypass authentic
CVE-2026-4255	A DLL search order hijacking vulnerability in Thermalright TR-VISION HOME on Windows (64-bit) allows a local attacker to escalate privileges via DLL side-loading. T the application is executed, which is always with administrative privileges, the malicious DLL is loaded instead of the legitimate library.\n\n\n\nThe application does the application's DLL search path and then cause the affected application to be executed. Once loaded, the malicious DLL runs with the same privileges as the app
CVE-2026-3558	Philips Hue Bridge HomeKit Accessory Protocol Transient Pairing Mode Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to authentication on the system. Was ZDI-CAN-28374.
CVE-2025-2274	Improper Neutralization of Input During Web Page Generation in Forcepoint Web Security (On-Prem) on Windows allows Stored XSS.This issue affects Web Security
CVE-2026-3557	Philips Hue Bridge hap_pair_verify_handler Sub-TLV Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-ad user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-2833
CVE-2026-29078	Lexbor is a web browser engine library. Prior to 2.7.0, the ISO-2022-JP encoder in Lexbor fails to reset the temporary size variable between iterations. The statemer
CVE-2026-3556	Philips Hue Bridge HomeKit Pair-Setup Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to ex the HomeKit service. Was ZDI-CAN-28326.
CVE-2026-3555	Philips Hue Bridge Zigbee Stack Custom Command Handler Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-ad size heap buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28276.
CVE-2026-3562	Philips Hue Bridge hk_hap Ed25519 Signature Verification Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to execute arbit
CVE-2026-23943	Improper Handling of Highly Compressed Data (Compression Bomb) vulnerability in Erlang OTP ssh (ssh_transport modules) allows Denial of Service via Resource D attacks Each SSH packet can decompress ~255 MB from 256 KB of wire data (1029:1 amplification ratio). Multiple packets can rapidly exhaust available memory, c
CVE-2026-1497	Incorrect resolving of namespaces in composite databases in Neo4j Enterprise edition prior to versions 2026.02 and 5.26.22 can lead to the following scenario: an

CVE-2026-23942	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP (ssh_sftpd module) allows Path Traversal. This vulnerabilit example, if root is set to /home/user1, paths like /home/user10 or /home/user1_backup would incorrectly be considered within the root. This issue affects OTP from
CVE-2026-0809	Use of a custom token encoding algorithm in Streamsoft Prestiż software allows the value of the KSeF (Krajowy System e-Faktur) token to be guessed after analyzi
CVE-2025-15060	claude-hovercraft executeClaudeCode Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary coc ZDI-CAN-27785.
CVE-2025-12690	Execution with unnecessary privileges in Forcepoint NGFW Engine allows local privilege escalation.This issue affects NGFW Engine through 6.10.19, through 7.3.0,
CVE-2026-2513	A vulnerability exists in Progress Flowmon ADS versions prior to 12.5.5 and 13.0.3, whereby an administrator who clicks a malicious link provided by an attacker m
CVE-2026-3013	Coppermine Photo Gallery in versions 1.6.09 through 1.6.27 is vulnerable to path traversal. Unauthenticated remote attacker is able to exploit a vulnerable endpoi
CVE-2025-14287	A command injection vulnerability exists in mlflow/mlflow versions before v3.7.0, specifically in the `mlflow/sagemaker/__init__.py` file at lines 161-167. The vulner cloud deployments.
CVE-2026-2514	In Progress Flowmon ADS versions prior to 12.5.5 and 13.0.3, a vulnerability exists whereby an adversary with access to Flowmon monitoring ports may craft malic
CVE-2025-11500	Tinycontrol devices such as tcPDU and LAN Controllers LK3.5, LK3.9 and LK4 have two separate authentication mechanisms - one solely for interface management This issue has been fixed in firmware versions: 1.36 (for tcPDU), 1.67 (for LK3.5 - hardware versions: 3.5, 3.6, 3.7 and 3.8), 1.75 (for LK3.9 - hardware version 3.9) a
CVE-2025-10685	Heap-based buffer overflow vulnerability in Softing Industrial Automation GmbH smartLink SW-PN and smartLink SW-HT (Webserver modules) allows overflow buffe
CVE-2025-10461	Global file reads caused by improper URL checks in webserver in Softing Industrial Automation GmbH smartLinks on docker (filesystem modules) allows file access.
CVE-2026-1668	The web interface on multiple Omada switches does not adequately validate certain external inputs, which may lead to out-of-bound memory access when process
CVE-2026-28384	An improper sanitization of the compression_algorithm parameter in Canonical LXD allows an authenticated, unprivileged user to execute commands as the LXD da
CVE-2025-15515	The authentication mechanism for a specific feature in the EasyShare module contains a vulnerability. If specific conditions are met on a local network, it can cause
CVE-2026-23940	Uncontrolled Resource Consumption vulnerability in hexpm hexpm/hexpm allows Excessive Allocation. Publishing an oversized package can cause Hex.pm to run o
CVE-2026-3839	Unraid Authentication Request Path Traversal Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected i
CVE-2026-23941	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in Erlang OTP (inets httpd module) allows HTTP Request Smuggling. This vul and allows front-end/back-end desynchronization, leaving attacker-controlled bytes queued as the start of the next request. This issue affects OTP from OTP 17.0 u
CVE-2026-3838	Unraid Update Request Path Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected install
CVE-2026-20892	Code injection vulnerability exists in MR-GM5L-S1 and MR-GM5A-L1, which may allow an attacker with administrative privileges to execute arbitrary commands.
CVE-2026-32274	Black is the uncompromising Python code formatter. Prior to 26.3.1, Black writes a cache file, the name of which is computed from various formatting options. The
CVE-2026-3237	In affected versions of Octopus Server it was possible for a low privileged user to manipulate an API request to change the signing key expiration and revocation tir
CVE-2026-3081	GStreamer H.266 Codec Parser Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary c vulnerability to execute code in the context of the current process. Was ZDI-CAN-28839.

CVE-2026-3023	Non-relational SQL injection vulnerability (NoSQLi) in the Wakyma web application, specifically in the endpoint 'vets.wakyma.com/pets/print-tags'. This vulnerability
CVE-2026-3022	Non-relational SQL injection vulnerability (NoSQLi) in the Wakyma web application, specifically in the endpoint 'vets.wakyma.com/hospitalization/generate-hospital
CVE-2026-3020	Identity based authorization bypass vulnerability (IDOR) that allows an attacker to modify the data of a legitimate user account, such as changing the victim's ema
CVE-2026-28254	A Missing Authorization vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an unauthenticated attacker to access sensitive information
CVE-2026-28255	A Use of Hard-coded Credentials vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive information and ta
CVE-2026-32251	Tolgee is an open-source localization platform. Prior to 3.166.3, the XML parsers used for importing Android XML resources (.xml) and .resx files don't disable exter
CVE-2026-32732	Lean 4 VS Code Extension is a Visual Studio Code extension for the Lean 4 proof assistant. Projects that use @leanprover/unicode-input-component are vulnerable
CVE-2026-29522	ZwickRoell Test Data Management versions prior to 3.0.8 contain a local file inclusion (LFI) vulnerability in the /server/node_upgrade_srv.js endpoint. An unauthent
CVE-2026-29777	Traefik is an HTTP reverse proxy and load balancer. Prior to 3.6.10, A tenant with write access to an HTTPRoute resource can inject backtick-delimited rule tokens i
CVE-2025-15552	Insufficient Session Expiration in Truesec’s LAPSWebUI before version 2.4 allows an attacker with access to a workstation to escalate their privileges via disclosure
CVE-2026-32720	The CTFer.io Monitoring component is in charge of the collection, process and storage of various signals (i.e. logs, metrics and distributed traces). Prior to 0.2.1, du
CVE-2026-27264	Rejected reason: This CVE ID was issued in error by its CVE Numbering Authority.
CVE-2026-27263	Rejected reason: This CVE ID was issued in error by its CVE Numbering Authority.
CVE-2025-15553	Non-working logout functionality in Truesec’s LAPSWebUI before version 2.4 allows an attacker with access to a workstation to escalate their privileges via disclosu
CVE-2025-15554	Browser caching of LAPS passwords in Truesec’s LAPSWebUI before version 2.4 allows an attacker with access to a workstation to escalate their privileges via discl
CVE-2025-15587	Tinycontrol devices such as tcPDU and LAN Controllers LK3.5, LK3.9 and LK4 allow a low privileged user to read an administrator's password by directly accessing a
CVE-2026-27261	Rejected reason: This CVE ID was issued in error by its CVE Numbering Authority.
CVE-2026-3024	Stored Cross-Site Scripting (XSS) vulnerability in the Wakyma web application, specifically in the endpoint 'vets.wakyma.com/configuracion/agenda/modelo-formul
CVE-2026-32261	Webhooks for Craft CMS plugin adds the ability to manage “webhooks” in Craft CMS, which will send GET or POST requests when certain events occur. From versio has been patched in version 3.2.0.
CVE-2026-3227	A command injection vulnerability was identified in TP-Link TL-WR802N v4, TL-WR841N v14, and TL-WR840N v6 due to improper neutralization of special elements
CVE-2025-69196	FastMCP is the standard framework for building MCP applications. Prior to version 2.14.2, the server does not properly respect the resource parameter submitted b
CVE-2026-29515	MiCode FileExplorer contains an authentication bypass vulnerability in the embedded SwiFTP FTP server component that allows network attackers to log in without

CVE-2026-29079	Lexbor is a web browser engine library. Prior to 2.7.0, a type-confusion vulnerability exists in Lexbor’s HTML fragment parser. When ns = UNDEF, a comment is cre
CVE-2026-3111	Insecure Direct Object Reference (IDOR) vulnerability in Campus Educativa specifically at the endpoint '/archivos/usuarios/[ID]/[username]/thumb_AAxAA.jpg' (trans doxxing.
CVE-2025-53517	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not assoc
CVE-2025-53815	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not assoc
CVE-2025-54758	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not assoc
CVE-2026-3110	Insecure Direct Object Reference (IDOR) vulnerability in Campus Educativa specifically at the endpoint '/administracion/admin_usuarios.cgi?filtro_estado=T&wAcci on the course ID via a manipulated URL.
CVE-2026-3086	GStreamer H.266 Codec Parser Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on code in the context of the current process. Was ZDI-CAN-28911.
CVE-2026-3085	GStreamer rtpqdm2depay Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code o execute code in the context of the current process. Was ZDI-CAN-28851.
CVE-2026-4092	Path Traversal in Clasp impacting versions < 3.2.0 allows a remote attacker to perform remote code execution via a malicious Google Apps Script project containin
CVE-2026-3084	GStreamer H.266 Codec Parser Integer Underflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on aff execute code in the context of the current process. Was ZDI-CAN-28910.
CVE-2026-3999	A broken access control may allow an authenticated user to perform a horizontal privilege escalation. The vulnerability only impacts specific configurations.
CVE-2026-28253	A Memory Allocation with Excessive Size Value vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an unauthenticated attacker to caus
CVE-2026-3083	GStreamer rtpqdm2depay Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affec leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28850.
CVE-2026-3644	The fix for CVE-2026-0672, which rejected control characters in http.cookies.Morsel, was incomplete. The Morsel.update(), |= operator, and unpickling paths were
CVE-2026-4224	When an Expat parser with a registered ElementDeclHandler parses an inline document type definition containing a deeply nested content model a C stack overflo
CVE-2026-3082	GStreamer JPEG Parser Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on a to execute code in the context of the current process. Was ZDI-CAN-28840.
CVE-2025-13462	The "tarfile" module would still apply normalization of AREGTYPE (\x00) blocks to DIRTYPE, even while processing a multi-block member such as GNUTYPE_LONGNA