SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 March 2026

Generated on 11 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-2026-30966	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.7 and 8.6.20, Parse Server's internal tables, which store Relation field mappings such as role memberships, can be directly accessed via the REST API or GraphQL API by any client using only the application key. No master key is required. An attacker can create, read, update, or delete records in any internal relationship table. Exploiting this allows the attacker to inject themselves into any Parse Role, gaining all permissions associated with that role, including full read, write, and delete access to classes protected by role-based Class-Level Permissions (CLP). Similarly, writing to any such table that backs a Relation field used in a pointerFields CLP bypasses that access control. This vulnerability is fixed in 9.5.2-alpha.7 and 8.6.20.	10.0	More Details
CVE-2025-48611	In DeviceId of DeviceId.java, there is a possible desync in persistence due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	10.0	More Details
CVE-2026-29128	IDC SFX2100 Satellite Receiver firmware ships with multiple daemon configuration files for routing components (e.g., zebra, bgpd, ospfd, and ripd) that are owned by root but world-readable. The configuration files (e.g., zebra.conf, bgpd.conf, ospfd.conf, ripd.conf) contain hardcoded or otherwise insecure plaintext passwords (including “enable”/privileged-mode credentials). A remote actor is able to abuse the reuse/hardcoded nature of these credentials to further access other systems in the network, gain a foothold on the satellite receiver or potentially locally privilege escalate.	10.0	More Details
CVE-2026-20079	A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and execute script files on an affected device to obtain root access to the underlying operating system. This vulnerability is due to an improper system process that is created at boot time. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute a variety of scripts and commands that allow root access to the device.	10.0	More Details
	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to execute arbitrary Java		

CVE-2026-20131	code as root on an affected device. This vulnerability is due to insecure deserialization of a user-supplied Java byte stream. An attacker could exploit this vulnerability by sending a crafted serialized Java object to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the device and elevate privileges to root. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced.	10.0	More Details
CVE-2026-30861	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. From version 0.2.5 to before version 0.2.10, an unauthenticated remote code execution (RCE) vulnerability exists in the MCP stdio configuration validation. The application allows unrestricted user registration, meaning any attacker can create an account and exploit the command injection flaw. Despite implementing a whitelist for allowed commands (npx, uvx) and blacklists for dangerous arguments and environment variables, the validation can be bypassed using the -p flag with npx node. This allows any attacker to execute arbitrary commands with the application's privileges, leading to complete system compromise. This issue has been patched in version 0.2.10.	9.9	More Details
CVE-2026-28466	OpenClaw versions prior to 2026.2.14 contain a vulnerability in the gateway in which it fails to sanitize internal approval fields in node.invoke parameters, allowing authenticated clients to bypass exec approval gating for system.run commands. Attackers with valid gateway credentials can inject approval control fields to execute arbitrary commands on connected node hosts, potentially compromising developer workstations and CI runners.	9.9	More Details
CVE-2026-24960	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Charety charety allows Using Malicious Files.This issue affects Charety: from n/a through < 2.0.2.	9.9	More Details
CVE-2026-22390	Improper Control of Generation of Code ('Code Injection') vulnerability in Builderall Builderall Builder for WordPress builderall-cheetah-for-wp allows Code Injection.This issue affects Builderall Builder for WordPress: from n/a through <= 3.0.1.	9.9	More Details
CVE-2025-68555	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Nutrie nutrie allows Upload a Web Shell to a Web Server.This issue affects Nutrie: from n/a through < 2.0.1.	9.9	More Details
CVE-2025-68554	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Keenarch keenarch allows Using Malicious Files.This issue affects Keenarch: from n/a through < 2.0.1.	9.9	More Details
CVE-2026-29789	Vito is a self-hosted web application that helps manage servers and deploy PHP applications into production servers. Prior to version 3.20.3, a missing authorization check in workflow site-creation actions allows an authenticated attacker with workflow write access in one project to create/manage sites on servers belonging to other projects by supplying a foreign server_id. This issue has been patched in version 3.20.3.	9.9	More Details
CVE-2026-30860	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.12, a remote code execution (RCE) vulnerability exists in the application's database query functionality. The validation system fails to recursively inspect child nodes within PostgreSQL array expressions and row expressions, allowing attackers to bypass SQL injection protections. By smuggling dangerous PostgreSQL functions inside these expressions and chaining them with large object operations and library loading capabilities, an unauthenticated attacker can achieve arbitrary code execution on the database server with database user privileges. This issue has been patched in version 0.2.12.	9.9	More Details
CVE-2025-68553	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Lendiz lendiz allows Upload a Web Shell to a Web Server.This issue affects Lendiz: from n/a through < 2.0.1.	9.9	More Details
CVE-2026-30957	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.21, OneUptime Synthetic Monitors allow a low-privileged authenticated project user to execute arbitrary commands on the oneuptime-probe server/container. The root cause is that untrusted Synthetic Monitor code is executed inside Node's vm while live host-realm Playwright browser and page objects are exposed to it. A malicious user can call Playwright APIs on the injected browser object and cause the probe to spawn an attacker-controlled executable. This is a server-side remote code execution issue. It does not require a separate vm sandbox escape. This vulnerability is fixed in 10.0.21.	9.9	More Details
CVE-2026-30956	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.21, a low-privileged user can bypass authorization and tenant isolation in OneUptime v10.0.20 and earlier by sending a forged is-multi-tenant-query header together with a controlled projectid header. Because the server trusts this client-supplied header, internal permission checks in BasePermission are skipped and tenant scoping is disabled. This allows attackers to access project data belonging to other tenants, read sensitive User fields via nested relations, leak plaintext	9.9	More Details

	resetPasswordToken, and reset the victim’s password and fully take over the account. This results in cross-tenant data exposure and full account takeover. This vulnerability is fixed in 10.0.21.		
CVE-2026-30887	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.18, OneUptime allows project members to run custom Playwright/JavaScript code via Synthetic Monitors to test websites. However, the system executes this untrusted user code inside the insecure Node.js vm module. By leveraging a standard prototype-chain escape (this.constructor.constructor), an attacker can bypass the sandbox, gain access to the underlying Node.js process object, and execute arbitrary system commands (RCE) on the oneuptime-probe container. Furthermore, because the probe holds database/cluster credentials in its environment variables, this directly leads to a complete cluster compromise. This vulnerability is fixed in 10.0.18.	9.9	More Details
CVE-2026-30921	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.20, OneUptime Synthetic Monitors allow low-privileged project users to submit custom Playwright code that is executed on the oneuptime-probe service. In the current implementation, this untrusted code is run inside Node's vm and is given live host Playwright objects such as browser and page. This creates a distinct server-side RCE primitive: the attacker does not need the classic this.constructor.constructor(...) sandbox escape. Instead, the attacker can directly use the injected Playwright browser object to reach browser.browserType().launch(...) and spawn an arbitrary executable on the probe host/container. This vulnerability is fixed in 10.0.20.	9.9	More Details
CVE-2025-40639	A SQL injection vulnerability has been found in Eventobot. This vulnerability allows an attacker to retrieve, create, update and delete databases through the 'promo_send' parameter in the '/assets/php/calculate_discount.php'.	9.8	More Details
CVE-2025-29165	An issue in D-Link DIR-1253 MESH V1.6.1684 allows an attacker to escalate privileges via the etc/shadow.sample component	9.8	More Details
CVE-2026-21536	Microsoft Devices Pricing Program Remote Code Execution Vulnerability	9.8	More Details
CVE-2026-28474	OpenClaw's Nextcloud Talk plugin versions prior to 2026.2.6 accept equality matching on the mutable actor.name display name field for allowlist validation, allowing attackers to bypass DM and room allowlists. An attacker can change their Nextcloud display name to match an allowlisted user ID and gain unauthorized access to restricted conversations.	9.8	More Details
CVE-2026-28470	OpenClaw versions prior to 2026.2.2 contain an exec approvals (must be enabled) allowlist bypass vulnerability that allows attackers to execute arbitrary commands by injecting command substitution syntax. Attackers can bypass the allowlist protection by embedding unescaped $() or backticks inside double-quoted strings to execute unauthorized commands.	9.8	More Details
CVE-2026-3843	Nefteprodukttekhnika BUK TS-G Gas Station Automation System 2.9.1 on Linux contains a SQL Injection vulnerability (CWE-89) in the system configuration module. A remote attacker can send specially crafted HTTP POST requests to the /php/request.php endpoint via the sql parameter in application/x-www-form-urlencoded data (e.g., action=do&sql=<query_here>&reload_driver=0) to execute arbitrary SQL commands and potentially achieve remote code execution.	9.8	More Details
CVE-2026-28292	`simple-git`, an interface for running git commands in any node.js application, has an issue in versions 3.15.0 through 3.32.2 that allows an attacker to bypass two prior CVE fixes (CVE-2022-25860 and CVE-2022-25912) and achieve full remote code execution on the host machine. Version 3.23.0 contains an updated fix for the vulnerability.	9.8	More Details
CVE-2026-28391	OpenClaw versions prior to 2026.2.2 fail to properly validate Windows cmd.exe metacharacters in allowlist-gated exec requests (non-default configuration), allowing attackers to bypass command approval restrictions. Remote attackers can craft command strings with shell metacharacters like & or %...% to execute unapproved commands beyond the allowlisted operations.	9.8	More Details
CVE-2026-27441	SEPPmail Secure Email Gateway before version 15.0.1 insufficiently neutralizes the PDF encryption password, allowing OS command execution.	9.8	More Details
CVE-2026-27944	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.3, the /api/backup endpoint is accessible without authentication and discloses the encryption keys required to decrypt the backup in the X-Backup-Security response header. This allows an unauthenticated attacker to download a full system backup containing sensitive data (user credentials, session tokens, SSL private keys, Nginx configurations) and decrypt it immediately. This issue has been patched in version 2.3.3.	9.8	More Details
CVE-2026-	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.3, an unauthenticated attacker can inject		More

27005	arbitrary SQL into queries executed against databases connected to Chartbrew (MySQL, PostgreSQL). This allows reading, modifying, or deleting data in those databases depending on the database user's privileges. This issue has been patched in version 4.8.3.	9.8	Details
CVE-2025-70233	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetEnableWizard.	9.8	More Details
CVE-2025-70232	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetMACFilter.	9.8	More Details
CVE-2025-70231	D-Link DIR-513 version 1.10 contains a critical-level vulnerability. When processing POST requests related to verification codes in /goform/formLogin, it enters /goform/getAuthCode but fails to filter the value of the FILECODE parameter, resulting in a path traversal vulnerability.	9.8	More Details
CVE-2025-70230	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetDDNS.	9.8	More Details
CVE-2025-70229	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSchedule.	9.8	More Details
CVE-2025-13476	Rakuten Viber Cloak mode in Android v25.7.2.0g and Windows v25.6.0.0–v25.8.1.0 uses a static and predictable TLS ClientHello fingerprint lacking extension diversity, allowing Deep Packet Inspection (DPI) systems to trivially identify and block proxy traffic, undermining censorship circumvention. (CWE-327)	9.8	More Details
CVE-2026-2599	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.7 via deserialization of untrusted input in the 'download_csv' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	9.8	More Details
CVE-2026-28501	WWBN AVideo is an open source video platform. Prior to version 24.0, an unauthenticated SQL Injection vulnerability exists in AVideo within the objects/videos.json.php and objects/video.php components. The application fails to properly sanitize the catName parameter when it is supplied via a JSON-formatted POST request body. Because JSON input is parsed and merged into $_REQUEST after global security checks are executed, the payload bypasses the existing sanitization mechanisms. This issue has been patched in version 24.0.	9.8	More Details
CVE-2026-28794	oRPC is an tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards. Prior to version 1.13.6, a prototype pollution vulnerability exists in the RPC JSON deserializer of the @orpc/client package. The vulnerability allows unauthenticated, remote attackers to inject arbitrary properties into the global Object.prototype. Because this pollution persists for the lifetime of the Node.js process and affects all objects, it can lead to severe security breaches, including authentication bypass, denial of service, and potentially Remote Code Execution. This issue has been patched in version 1.13.6.	9.8	More Details
CVE-2026-28785	Ghostfolio is an open source wealth management software. Prior to version 2.244.0, by bypassing symbol validation, an attacker can execute arbitrary SQL commands via the getHistorical() method, potentially allowing them to read, modify, or delete sensitive financial data for all users in the database. This issue has been patched in version 2.244.0.	9.8	More Details
CVE-2026-24713	Improper Input Validation vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.0.0 before 1.3.7, from 2.0.0 before 2.0.7. Users are recommended to upgrade to version 1.3.7 or 2.0.7, which fixes the issue.	9.8	More Details
CVE-2026-24015	A vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.0.0 before 1.3.7, from 2.0.0 before 2.0.7. Users are recommended to upgrade to version 1.3.7 or 2.0.7, which fixes the issue.	9.8	More Details
CVE-2026-3630	Delta Electronics COMMGR2 has Stack-based Buffer Overflow vulnerability.	9.8	More Details
CVE-2026-3703	A flaw has been found in Wavlink NU516U1 251208. This affects the function sub_401A10 of the file /cgi-bin/login.cgi. Executing a manipulation of the argument ipaddr can lead to out-of-bounds write. The attack may be performed from remote. The exploit has been published and may be used. Upgrading the affected component is recommended. The vendor was contacted early, responded in	9.8	More Details

	a very professional manner and quickly released a fixed version of the affected product.		
CVE-2026-30909	Crypt::NaCl::Sodium versions through 2.002 for Perl has potential integer overflows. bin2hex, encrypt, aes256gcm_encrypt_afternm and seal functions do not check that output size will be less than SIZE_MAX, which could lead to integer wraparound causing an undersized output buffer. Encountering this issue is unlikely as the message length would need to be very large. For bin2hex() the bin_len would have to be > SIZE_MAX / 2 For encrypt() the msg_len would need to be > SIZE_MAX - 16U For aes256gcm_encrypt_afternm() the msg_len would need to be > SIZE_MAX - 16U For seal() the enc_len would need to be > SIZE_MAX - 64U	9.8	More Details
CVE-2026-30863	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.10 and 9.5.0-alpha.11, the Google, Apple, and Facebook authentication adapters use JWT verification to validate identity tokens. When the adapter's audience configuration option is not set (clientId for Google/Apple, appIds for Facebook), JWT verification silently skips audience claim validation. This allows an attacker to use a validly signed JWT issued for a different application to authenticate as any user on the target Parse Server. This issue has been patched in versions 8.6.10 and 9.5.0-alpha.11.	9.8	More Details
CVE-2026-0953	The Tutor LMS Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 3.9.5 via the Social Login addon. This is due to the plugin failing to verify that the email provided in the authentication request matches the email from the validated OAuth token. This makes it possible for unauthenticated attackers to log in as any existing user, including administrators, by supplying a valid OAuth token from their own account along with the victim's email address.	9.8	More Details
CVE-2026-2331	An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the HTTP-based file access feature, allowing access without authentication. This includes device parameter files, enabling an attacker to read and modify application settings, including customer-defined passwords. Additionally, exposure of the custom application directory may allow execution of arbitrary Lua code within the sandboxed AppEngine environment.	9.8	More Details
CVE-2026-29058	AVideo is a video-sharing Platform software. Prior to version 7.0, an unauthenticated attacker can execute arbitrary OS commands on the server by injecting shell command substitution into the base64Url GET parameter. This can lead to full server compromise, data exfiltration (e.g., configuration secrets, internal keys, credentials), and service disruption. This issue has been patched in version 7.0.	9.8	More Details
CVE-2026-29042	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.15.20, the Nuclio Shell Runtime component contains a command injection vulnerability in how it processes user-supplied arguments. When a function is invoked via HTTP, the runtime reads the X-Nuclio-Arguments header and directly incorporates its value into shell commands without any validation or sanitization. This issue has been patched in version 1.15.20.	9.8	More Details
CVE-2026-28802	Authlib is a Python library which builds OAuth and OpenID Connect servers. From version 1.6.5 to before version 1.6.7, previous tests involving passing a malicious JWT containing alg: none and an empty signature was passing the signature verification step without any changes to the application code when a failure was expected.. This issue has been patched in version 1.6.7.	9.8	More Details
CVE-2025-41709	[PROBLEMTYPE] in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] on [PLATFORMS] allows [ATTACKER] to [IMPACT] via [VECTOR]	9.8	More Details
CVE-2025-56422	A deserialization vulnerability in LimeSurvey before v6.15.0+250623 allows a remote attacker to execute arbitrary code on the server.	9.8	More Details
CVE-2026-28795	OpenChatBI is an intelligent chat-based BI tool powered by large language models, designed to help users query, analyze, and visualize data through natural language conversations. Prior to version 0.2.2, the save_report tool in openchatbi/tool/save_report.py suffers from a critical path traversal vulnerability due to insufficient input sanitization of the file_format parameter. This issue has been patched in version 0.2.2.	9.8	More Details
CVE-2026-28438	CocoIndex is a data transformation framework for AI. Prior to version 0.3.34, the Doris target connector didn't verify the configured table name before creating some SQL statements (ALTER TABLE). So, in the application code, if the table name is provided by an untrusted upstream, it expose vulnerability to SQL injection when target schema change. This issue has been patched in version 0.3.34.	9.8	More Details
	The PowerPack for LearnDash WordPress plugin before 1.3.0 does not have authorization and CRSF		

CVE-2026-2446	checks in an AJAX action, allowing unauthenticated users to update arbitrary WordPress options (such as default_role etc) and create arbitrary admin users	9.8	More Details
CVE-2026-2743	Arbitrary File Write via Path Traversal upload to Remote Code Execution in SeppMail User Web Interface. The affected feature is the large file transfer (LFT). This issue affects SeppMail: 15.0.2.1 and before	9.8	More Details
CVE-2026-28775	An unauthenticated Remote Code Execution (RCE) vulnerability exists in the SNMP service of International Datacasting Corporation (IDC) SFX Series SuperFlex SatelliteReceiver. The deployment insecurely provisions the \`private\` SNMP community string with read/write access by default. Because the SNMP agent runs as root, an unauthenticated remote attacker can utilize \`NET-SNMP-EXTEND-MIB\` directives, abusing the fact that the system runs a vulnerable version of net-snmp pre 5.8, to execute arbitrary operating system commands with root privileges.	9.8	More Details
CVE-2026-22474	Deserialization of Untrusted Data vulnerability in ThemeREX Equestrian Centre equestrian-centre allows Object Injection.This issue affects Equestrian Centre: from n/a through <= 1.5.	9.8	More Details
CVE-2026-23767	ESC/POS, a printer control language designed by Seiko Epson Corporation, lacks mechanisms for user authentication and command authorization, does not provide controls to restrict sources or destinations of network communication, and transmits commands without encryption or integrity protection.	9.8	More Details
CVE-2026-22497	Deserialization of Untrusted Data vulnerability in AncoraThemes Jardi jardi allows Object Injection.This issue affects Jardi: from n/a through <= 1.7.2.	9.8	More Details
CVE-2026-22475	Deserialization of Untrusted Data vulnerability in axiomthemes Estate estate allows Object Injection.This issue affects Estate: from n/a through <= 1.3.4.	9.8	More Details
CVE-2026-22454	Deserialization of Untrusted Data vulnerability in ThemeREX Solaris solaris allows Object Injection.This issue affects Solaris: from n/a through <= 2.5.	9.8	More Details
CVE-2026-22453	Deserialization of Untrusted Data vulnerability in ThemeREX Pets Club petclub allows Object Injection.This issue affects Pets Club: from n/a through <= 2.3.	9.8	More Details
CVE-2026-22451	Deserialization of Untrusted Data vulnerability in AncoraThemes Handyman handyman-services allows Object Injection.This issue affects Handyman: from n/a through <= 1.4.	9.8	More Details
CVE-2025-54001	Deserialization of Untrusted Data vulnerability in ThemeREX Classter classter allows Object Injection.This issue affects Classter: from n/a through <= 2.5.	9.8	More Details
CVE-2026-3381	Compress::Raw::Zlib versions through 2.219 for Perl use potentially insecure versions of zlib. Compress::Raw::Zlib includes a copy of the zlib library. Compress::Raw::Zlib version 2.220 includes zlib 1.3.2, which addresses findings fron the 7ASecurity audit of zlib. The includes fixs for CVE-2026-27171.	9.8	More Details
CVE-2026-3257	UnQLite versions through 0.06 for Perl uses a potentially insecure version of the UnQLite library. UnQLite for Perl embeds the UnQLite library. Version 0.06 and earlier of the Perl module uses a version of the library from 2014 that may be vulnerable to a heap-based overflow.	9.8	More Details
CVE-2025-70218	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via POST to the goform/formAdvFirewall component.	9.8	More Details
CVE-2025-40926	Plack::Middleware::Session::Simple versions through 0.04 for Perl generates session ids insecurely. The default session id generator returns a SHA-1 hash seeded with the built-in rand function, the epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems. Plack::Middleware::Session::Simple is intended to be compatible with Plack::Middleware::Session, which had a similar security issue CVE-2025-40923.	9.8	More Details
CVE-2025-70220	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formAutoDetecWAN_wizard4.	9.8	More Details
CVE-2025-70222	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formLogin,goform/getAuthCode.	9.8	More Details
CVE-2025-70225	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curtime parameter to the goform/formEasySetupWWConfig component	9.8	More Details
CVE-2025-	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to		More

70221	goform/formLogin.	9.8	Details
CVE-2025-46108	D-link Dir-513 A1FW110 is vulnerable to Buffer Overflow in the function formTcpipSetup.	9.8	More Details
CVE-2025-70219	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the goform/formDeviceReboot.	9.8	More Details
CVE-2025-70226	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formEasySetupWizard.	9.8	More Details
CVE-2026-22501	Deserialization of Untrusted Data vulnerability in axiomthemes Mounthood mounthood allows Object Injection.This issue affects Mounthood: from n/a through <= 1.3.2.	9.8	More Details
CVE-2025-70223	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formAdvNetwork.	9.8	More Details
CVE-2026-28043	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Healer - Doctor, Clinic & Medical WordPress Theme healer allows PHP Local File Inclusion.This issue affects Healer - Doctor, Clinic & Medical WordPress Theme: from n/a through <= 1.0.0.	9.8	More Details
CVE-2026-28074	Deserialization of Untrusted Data vulnerability in ThemeREX Pizza House pizzahouse allows Object Injection.This issue affects Pizza House: from n/a through <= 1.4.0.	9.8	More Details
CVE-2025-66944	SQL Injection vulnerability in vran-dev databaseir v.1.0.7 and before allows a remote attacker to execute arbitrary code via the query parameter in the search API endpoint	9.8	More Details
CVE-2026-27439	Deserialization of Untrusted Data vulnerability in ThemeREX Dentario dentario allows Object Injection.This issue affects Dentario: from n/a through <= 1.5.	9.8	More Details
CVE-2026-27983	Incorrect Privilege Assignment vulnerability in designthemes LMS Elementor Pro lms-elementor-pro allows Privilege Escalation.This issue affects LMS Elementor Pro: from n/a through <= 1.0.4.	9.8	More Details
CVE-2026-27437	Deserialization of Untrusted Data vulnerability in ThemeREX Tennis Club tennis-sportclub allows Object Injection.This issue affects Tennis Club: from n/a through <= 1.2.3.	9.8	More Details
CVE-2025-59786	2N Access Commander version 3.4.2 and prior improperly invalidates session tokens, allowing multiple session cookies to remain active after logout in web application.	9.8	More Details
CVE-2026-27417	Deserialization of Untrusted Data vulnerability in SeventhQueen Sweet Date sweetdate allows Object Injection.This issue affects Sweet Date: from n/a through < 4.0.1.	9.8	More Details
CVE-2026-26478	A shell command injection vulnerability in Mobvoi Tichome Mini smart speaker 012-18853 and 027-58389 allows remote attackers to send a specially crafted UDP datagram and execute arbitrary shell code as the root account.	9.8	More Details
CVE-2026-27438	Deserialization of Untrusted Data vulnerability in ThemeREX Kingler kingler allows Object Injection.This issue affects Kingler: from n/a through <= 1.7.	9.8	More Details
CVE-2026-28105	Deserialization of Untrusted Data vulnerability in ThemeREX Good Energy goodenergy allows Object Injection.This issue affects Good Energy: from n/a through <= 1.7.7.	9.8	More Details
CVE-2025-66678	An issue in the HwRwDrv.sys component of Nil Hardware Editor Hardware Read & Write Utility v1.25.11.26 and earlier allows attackers to execute arbitrary read and write operations via a crafted request.	9.8	More Details
CVE-2026-27389	Authentication Bypass Using an Alternate Path or Channel vulnerability in designthemes WeDesignTech Ultimate Booking Addon wedesigntech-ultimate-booking-addon allows Authentication Abuse.This issue affects WeDesignTech Ultimate Booking Addon: from n/a through <= 1.0.1.	9.8	More Details
CVE-2026-28495	GetSimple CMS is a content management system. The massiveAdmin plugin (v6.0.3) bundled with GetSimpleCMS-CE v3.3.22 allows an authenticated administrator to overwrite the gsconfig.php configuration file with arbitrary PHP code via the gsconfig editor module. The form lacks CSRF protection, enabling a remote unauthenticated attacker to exploit this via Cross-Site Request Forgery against a logged-in admin, achieving Remote Code Execution (RCE) on the web server.	9.6	More Details
CVE-2026-3545	Insufficient data validation in Navigation in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details

CVE-2026-28536	Authentication bypass vulnerability in the device authentication module. Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	9.6	More Details
CVE-2025-40943	Affected devices do not properly sanitize contents of trace files. This could allow an attacker to inject code through social engineering a legitimate user to import a specially crafted trace file	9.6	More Details
CVE-2026-30240	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.31.5 and earlier, a path traversal vulnerability in the PWA (Progressive Web App) ZIP processing endpoint (POST /api/pwa/process-zip) allows an authenticated user with builder privileges to read arbitrary files from the server filesystem, including /proc/1/environ which contains all environment variables — JWT secrets, database credentials, encryption keys, and API tokens. The server reads attacker-specified files via unsanitized path.join() with user-controlled input from icons.json inside the uploaded ZIP, then uploads the file contents to the object store (MinIO/S3) where they can be retrieved through signed URLs. This results in complete platform compromise as all cryptographic secrets and service credentials are exfiltrated in a single request.	9.6	More Details
CVE-2025-69969	A lack of authentication and authorization mechanisms in the Bluetooth Low Energy (BLE) communication protocol of SRK Powertech Pvt Ltd Pebble Prism Ultra v2.9.2 allows attackers to reverse engineer the protocol and execute arbitrary commands on the device without establishing a connection. This is exploitable over Bluetooth Low Energy (BLE) proximity (Adjacent), requiring no physical contact with the device. Furthermore, the vulnerability is not limited to arbitrary commands but includes cleartext data interception and unauthenticated firmware hijacking via OTA services.	9.6	More Details
CVE-2026-26051	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-26288	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-1678	dns_unpack_name() caches the buffer tailroom once and reuses it while appending DNS labels. As the buffer grows, the cached size becomes incorrect, and the final null terminator can be written past the buffer. With assertions disabled (default), a malicious DNS response can trigger an out-of-bounds write when CONFIG_DNS_RESOLVER is enabled.	9.4	More Details
CVE-2026-2330	An attacker may access restricted filesystem areas on the device via the CROWN REST interface due to incomplete whitelist enforcement. Certain directories intended for internal testing were not covered by the whitelist and are accessible without authentication. An unauthenticated attacker could place a manipulated parameter file that becomes active after a reboot, allowing modification of critical device settings, including network configuration and application parameters.	9.4	More Details
CVE-2025-69614	Incorrect Access Control via activation token reuse on the password-reset endpoint allowing unauthorized password resets and full account takeover. Affected Product: Deutsche Telekom AG Telekom Account Management Portal, versions before 2025-10-27, fixed 2025-10-31.	9.4	More Details
CVE-2026-28446	OpenClaw versions prior to 2026.2.1 with the voice-call extension installed and enabled contain an authentication bypass vulnerability in inbound allowlist policy validation that accepts empty caller IDs and uses suffix-based matching instead of strict equality. Remote attackers can bypass inbound access controls by placing calls with missing caller IDs or numbers ending with allowlisted digits to reach the voice-call agent and execute tools.	9.4	More Details
CVE-2026-22552	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.	9.4	More Details
CVE-2026-	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in loopus WP Attractive Donations System - Easy Stripe & Paypal donations	9.3	More

28115	WP_AttractiveDonationsSystem allows Blind SQL Injection.This issue affects WP Attractive Donations System - Easy Stripe & Paypal donations: from n/a through <= 1.25.		Details
CVE-2026-30869	SiYuan is a personal knowledge management system. Prior to 3.5.10, a path traversal vulnerability in the /export endpoint allows an attacker to read arbitrary files from the server filesystem. By exploiting double-encoded traversal sequences, an attacker can access sensitive files such as conf/conf.json, which contains secrets including the API token, cookie signing key, and workspace access authentication code. Leaking these secrets may enable administrative access to the SiYuan kernel API, and in certain deployment scenarios could potentially be chained into remote code execution (RCE). This vulnerability is fixed in 3.5.10.	9.3	More Details
CVE-2026-29183	SiYuan is a personal knowledge management system. Prior to version 3.5.9, an unauthenticated reflected XSS vulnerability exists in the dynamic icon API endpoint "GET /api/icon/getDynamicIcon" when type=8, attacker-controlled content is embedded into SVG output without escaping. Because the endpoint is unauthenticated and returns image/svg+xml, a crafted URL can inject executable SVG/HTML event handlers (for example onerror) and run JavaScript in the SiYuan web origin. This can be chained to perform authenticated API actions and exfiltrate sensitive data when a logged-in user opens the malicious link. This issue has been patched in version 3.5.9.	9.3	More Details
CVE-2025-70948	A host header injection vulnerability in the mailer component of @perfood/couch-auth v0.26.0 allows attackers to obtain reset tokens and execute an account takeover via spoofing the HTTP Host header.	9.3	More Details
CVE-2025-69338	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in don-themes Riode Core riode-core allows Blind SQL Injection.This issue affects Riode Core: from n/a through <= 1.6.26.	9.3	More Details
CVE-2026-25921	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, overwritable LFS object across different repos leads to supply-chain attack, all LFS objects are vulnerable to be maliciously overwritten by malicious attackers. This issue has been patched in version 0.14.2.	9.3	More Details
CVE-2026-29191	ZITADEL is an open source identity management platform. From version 4.0.0 to 4.11.1, a vulnerability in Zitadel's login V2 interface was discovered that allowed a possible account takeover via XSS in /saml-post Endpoint. This issue has been patched in version 4.12.0.	9.3	More Details
CVE-2026-28680	Ghostfolio is an open source wealth management software. Prior to version 2.245.0, an attacker can exploit the manual asset import feature to perform a full-read SSRF, allowing them to exfiltrate sensitive cloud metadata (IMDS) or probe internal network services. This issue has been patched in version 2.245.0.	9.3	More Details
CVE-2025-11158	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.6, including 9.3.x and 8.3.x, do not restrict Groovy scripts in new PRPT reports published by users, allowing insertion of arbitrary scripts and leading to a RCE.	9.1	More Details
CVE-2026-28783	Craft is a content management system (CMS). Prior to 5.9.0-beta.1 and 4.17.0-beta.1, Craft CMS implements a blocklist to prevent potentially dangerous PHP functions from being called via Twig non-Closure arrow functions. In order to be able to successfully execute this attack, you need to either have allowAdminChanges enabled on production, or a compromised admin account, or an account with access to the System Messages utility. Several PHP functions are not included in the blocklist, which could allow malicious actors with the required permissions to execute various types of payloads, including RCEs, arbitrary file reads, SSRFs, and SSTIs. This vulnerability is fixed in 5.9.0-beta.1 and 4.17.0-beta.1.	9.1	More Details
CVE-2026-27685	SAP NetWeaver Enterprise Portal Administration is vulnerable if a privileged user uploads untrusted or malicious content that, upon deserialization, could result in a high impact on the confidentiality, integrity, and availability of the host system.	9.1	More Details
CVE-2025-69615	Incorrect Access Control via missing 2FA rate-limiting allowing unlimited brute-force retries and full MFA bypass with no user interaction required. Affected Product: Deutsche Telekom AG Telekom Account Management Portal, versions before 2025-10-24, fixed 2025-11-03.	9.1	More Details
CVE-2026-28697	Craft is a content management system (CMS). Prior to 4.17.0-beta.1 and 5.9.0-beta.1, an authenticated administrator can achieve Remote Code Execution (RCE) by injecting a Server-Side Template Injection (SSTI) payload into Twig template fields (e.g., Email Templates). By calling the craft.app.fs.write() method, an attacker can write a malicious PHP script to a web-accessible directory and subsequently access it via the browser to execute arbitrary system commands. This vulnerability is fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	9.1	More Details
CVE-2026-	The Login with Salesforce WordPress plugin through 1.0.2 does not validate that users are allowed		More

2418	to login through Salesforce, allowing unauthenticated users to be authenticated as any user (such as admin) by simply knowing the email	9.1	Details
CVE-2026-31816	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.31.4 and earlier, the Budibase server's authorized() middleware that protects every server-side API endpoint can be completely bypassed by appending a webhook path pattern to the query string of any request. The isWebhookEndpoint() function uses an unanchored regex that tests against ctx.request.url, which in Koa includes the full URL with query parameters. When the regex matches, the authorized() middleware immediately calls return next(), skipping all authentication, authorization, role checks, and CSRF protection. This means a completely unauthenticated, remote attacker can access any server-side API endpoint by simply appending ?/webhooks/trigger (or any webhook pattern variant) to the URL.	9.1	More Details
CVE-2026-29065	changedetection.io is a free open source web page change detection tool. Prior to version 0.54.4, a Zip Slip vulnerability in the backup restore functionality allows arbitrary file overwrite via path traversal in uploaded ZIP archives. This issue has been patched in version 0.54.4.	9.1	More Details
CVE-2026-28114	Unrestricted Upload of File with Dangerous Type vulnerability in firassaidi WooCommerce License Manager fs-license-manager allows Upload a Web Shell to a Web Server.This issue affects WooCommerce License Manager: from n/a through <= 7.0.6.	9.1	More Details
CVE-2026-29188	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Prior to version 2.61.1, a broken access control vulnerability in the TUS protocol DELETE endpoint allows authenticated users with only Create permission to delete arbitrary files and directories within their scope, bypassing the intended Delete permission restriction. Any multi-user deployment where administrators explicitly restrict file deletion for certain users is affected. This issue has been patched in version 2.61.1.	9.1	More Details
CVE-2026-23802	Unrestricted Upload of File with Dangerous Type vulnerability in Jordy Meow AI Engine ai-engine allows Using Malicious Files.This issue affects AI Engine: from n/a through <= 3.3.2.	9.1	More Details
CVE-2025-41765	Due to insufficient authorization enforcement, an unauthorized remote attacker can exploit the wwwupload.cgi endpoint to upload and apply arbitrary data. This includes, but is not limited to, contact images, HTTPS certificates, system backups for restoration, server peer configurations, and BACnet/SC server certificates and keys.	9.1	More Details
CVE-2024-57854	Net::NSCA::Client versions through 0.009002 for Perl uses a poor random number generator. Version v0.003 switched to use Data::Rand::Obscure instead of Crypt::Random for generation of a random initialisation vectors. Data::Rand::Obscure uses Perl's built-in rand() function, which is not suitable for cryptographic functions.	9.1	More Details
CVE-2026-24457	An unsafe parsing of OpenMQ's configuration, allows a remote attacker to read arbitrary files from a MQ Broker's server. A full exploitation could read unauthorized files of the OpenMQ’s host OS. In some scenarios RCE could be achieved.	9.1	More Details
CVE-2025-40931	Apache::Session::Generate::MD5 versions through 1.94 for Perl create insecure session id. Apache::Session::Generate::MD5 generates session ids insecurely. The default session id generator returns a MD5 hash seeded with the built-in rand() function, the epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems.	9.1	More Details
CVE-2026-30832	Soft Serve is a self-hostable Git server for the command line. From version 0.6.0 to before version 0.11.4, an authenticated SSH user can force the server to make HTTP requests to internal/private IP addresses by running repo import with a crafted --lfs-endpoint URL. The initial batch request is blind (the response from a metadata endpoint won't parse as valid LFS JSON), but an attacker hosting a fake LFS server can chain this into full read access to internal services by returning download URLs that point at internal targets. This issue has been patched in version 0.11.4.	9.1	More Details
CVE-2026-29000	pac4j-jwt versions prior to 4.5.9, 5.7.9, and 6.3.3 contain an authentication bypass vulnerability in JwtAuthenticator when processing encrypted JWTs that allows remote attackers to forge authentication tokens. Attackers who possess the server's RSA public key can create a JWE-wrapped PlainJWT with arbitrary subject and role claims, bypassing signature verification to authenticate as any user including administrators.	9.1	More Details
CVE-2025-41764	Due to insufficient authorization enforcement, an unauthorized remote attacker can exploit the wwwupdate.cgi endpoint to upload and apply arbitrary updates.	9.1	More Details
	Chamilo is a learning management system. Prior to version 1.11.34, there is a stored cross-site		

CVE-2025-59542	scripting (XSS) vulnerability. By injecting malicious JavaScript into the course learning path Settings field, an attacker with a low-privileged account (e.g., trainer) can execute arbitrary JavaScript code in the context of any other user viewing the course information page, including administrators. This allows an attacker to exfiltrate sensitive session cookies or tokens, resulting in account takeover (ATO) of higher-privileged users. This issue has been patched in version 1.11.34.	9.0	More Details
CVE-2026-27384	Improper Validation of Specified Quantity in Input vulnerability in BoldGrid W3 Total Cache w3-total-cache allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects W3 Total Cache: from n/a through <= 2.9.1.	9.0	More Details
CVE-2025-55208	Chamilo is a learning management system. Versions prior to 1.11.34 have a Stored XSS through insecure file uploads in `Social Networks`. Through it, a low-privilege user can execute arbitrary code in the admin user inbox, allowing takeover of the admin account. Version 1.11.34 fixes the issue.	9.0	More Details
CVE-2026-27984	Improper Control of Generation of Code ('Code Injection') vulnerability in Marketing Fire Widget Options widget-options allows Code Injection.This issue affects Widget Options: from n/a through <= 4.1.3.	9.0	More Details
CVE-2026-27825	MCP Atlassian is a Model Context Protocol (MCP) server for Atlassian products (Confluence and Jira). Prior to version 0.17.0, the `confluence_download_attachment` MCP tool accepts a `download_path` parameter that is written to without any directory boundary enforcement. An attacker who can call this tool and supply or access a Confluence attachment with malicious content can write arbitrary content to any path the server process has write access to. Because the attacker controls both the write destination and the written content (via an uploaded Confluence attachment), this constitutes for arbitrary code execution (for example, writing a valid cron entry to `/etc/cron.d/` achieves code execution within one scheduler cycle with no server restart required). Version 0.17.0 fixes the issue.	9.0	More Details
CVE-2026-30862	Appsmith is a platform to build admin panels, internal tools, and dashboards. Prior to 1.96, a Critical Stored XSS vulnerability exists in the Table Widget (TableWidgetV2). The root cause is a lack of HTML sanitization in the React component rendering pipeline, allowing malicious attributes to be interpolated into the DOM. By leveraging the "Invite Users" feature, an attacker with a regular user account (user@gmail.com) can force a System Administrator to execute a high-privileged API call (/api/v1/admin/env), resulting in a Full Administrative Account Takeover. This vulnerability is fixed in 1.96.	9.0	More Details
CVE-2025-59543	Chamilo is a learning management system. Prior to version 1.11.34, there is a stored cross-site scripting (XSS) vulnerability. By injecting malicious JavaScript into the course description field, an attacker with a low-privileged account (e.g., trainer) can execute arbitrary JavaScript code in the context of any other user viewing the course information page, including administrators. This allows an attacker to exfiltrate sensitive session cookies or tokens, resulting in account takeover (ATO) of higher-privileged users. This issue has been patched in version 1.11.34.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-25737	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.24.0 and earlier, an arbitrary file upload vulnerability exists even though file extension restrictions are configured. The restriction is enforced only at the UI level. An attacker can bypass these restrictions and upload malicious files.	8.9	More Details
CVE-2026-30934	FileBrowser Quantum is a free, self-hosted, web-based file manager. Prior to 1.3.1-beta and 1.2.2-stable, Stored XSS is possible via share metadata fields (e.g., title, description) that are rendered into HTML for /public/share/<hash> without context-aware escaping. The server uses text/template instead of html/template, allowing injected scripts to execute when victims visit the share URL. This vulnerability is fixed in 1.3.1-beta and 1.2.2-stable.	8.9	More Details
CVE-2026-3804	A security flaw has been discovered in Tenda i3 1.0.0.6(2204). This vulnerability affects the function formWifiMacFilterSet of the file /goform/WifiMacFilterSet. The manipulation of the argument index results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-	A vulnerability was determined in Tenda F453 1.0.0.3/1.If. This issue affects the function fromSetCfm of the file /goform/setcfm. This manipulation of the argument funcname/funcpara1 causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed	8.8	More Details

3728	and may be utilized.		
CVE-2026-3700	A weakness has been identified in UTT HiPER 810G up to 1.7.7-171114. Affected is the function strcpy of the file /goform/formConfigDnsFilterGlobal. This manipulation causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-25172	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-3715	A vulnerability was found in Wavlink WL-WN579X3-C 231124. This affects the function sub_40139C of the file /cgi-bin/firewall.cgi. Performing a manipulation of the argument del_flag results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. Upgrading to version 20260226 is able to mitigate this issue. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	8.8	More Details
CVE-2026-3726	A vulnerability has been found in Tenda F453 1.0.0.3. This affects the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-3727	A vulnerability was found in Tenda F453 1.0.0.3. This vulnerability affects the function sub_3C6C0 of the file /goform/QuickIndex. The manipulation of the argument mit_linktype/PPPOEPassword results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-3729	A vulnerability was identified in Tenda F453 1.0.0.3/3.As. Impacted is the function fromPptpUserAdd of the file /goform/PPTPDClient. Such manipulation of the argument username/opttype leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-25177	Improper restriction of names for files and other resources in Active Directory Domain Services allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-24283	Heap-based buffer overflow in Windows File Server allows an authorized attacker to elevate privileges locally.	8.8	More Details
CVE-2026-3732	A security vulnerability has been detected in Tenda F453 1.0.0.3. This affects the function strcpy of the file /goform/exeCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-3801	A vulnerability was found in Tenda i3 1.0.0.6(2204). Affected by this vulnerability is the function formSetAutoPing of the file /goform/setAutoPing. Performing a manipulation of the argument ping1/ping2 results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-23669	Use after free in Windows Print Spooler Components allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-3802	A vulnerability was determined in Tenda i3 1.0.0.6(2204). Affected by this issue is the function formexeCommand of the file /goform/exeCommand. Executing a manipulation of the argument cmdinput can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-3803	A vulnerability was identified in Tenda i3 1.0.0.6(2204). This affects the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-3699	A security flaw has been discovered in UTT HiPER 810G up to 1.7.7-171114. This impacts the function strcpy of the file /goform/formRemoteControl. The manipulation results in buffer overflow. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details

CVE-2026-3679	A vulnerability was identified in Tenda FH451 1.0.0.9. Affected by this vulnerability is the function formQuickIndex of the file /goform/QuickIndex. Such manipulation of the argument mit_linktype/PPPOEPassword leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-3698	A vulnerability was identified in UTT HiPER 810G up to 1.7.7-171114. This affects the function strcpy of the file /goform/NTP. The manipulation leads to buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-22627	A buffer copy without checking size of input ('classic buffer overflow') vulnerability in Fortinet FortiSwitchAXFixed 1.0.0 through 1.0.1 may allow an unauthenticated attacker within the same adjacent network to execute unauthorized code or commands on the device via sending a crafted LLDP packet.	8.8	More Details
CVE-2026-3678	A vulnerability was determined in Tenda FH451 1.0.0.9. Affected is the function sub_3C434 of the file /goform/AdvSetWan. This manipulation of the argument wanmode/PPPOEPassword causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-25188	Heap-based buffer overflow in Windows Telephony Service allows an unauthorized attacker to elevate privileges over an adjacent network.	8.8	More Details
CVE-2026-3677	A vulnerability was found in Tenda FH451 1.0.0.9. This impacts the function fromSetCfm of the file /goform/setcfm. The manipulation of the argument funcname/funcpara1 results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-30855	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.3.2, an authorization bypass in tenant management endpoints of WeKnora application allows any authenticated user to read, modify, or delete any tenant by ID. Since account registration is open to the public, this vulnerability allows any unauthenticated attacker to register an account and subsequently exploit the system. This enables cross-tenant account takeover and destruction, making the impact critical. This issue has been patched in version 0.3.2.	8.8	More Details
CVE-2026-1720	The WowOptin: Next-Gen Popup Maker – Create Stunning Popups and Optins for Lead Generation plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the 'install_and_active_plugin' function in all versions up to, and including, 1.4.24. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate arbitrary plugins.	8.8	More Details
CVE-2026-26106	Improper input validation in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-26111	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-8899	The Paid Videochat Turnkey Site – HTML5 PPV Live Webcams plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 7.3.20. This is due to videowhisper_register_form() function not restricting user roles that can be set during registration. This makes it possible for authenticated attackers, with Author-level access and above, to create posts/pages with the registration form and administrator set as the role and subsequently use that form to register an administrator account. This can also be exploited by contributors, but is far less likely to be successful because an administrator would need to approve the form with the administrator role for the attack to be successful.	8.8	More Details
CVE-2026-26114	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-26115	Improper validation of specified type of input in SQL Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-26116	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details

CVE-2026-26118	Server-side request forgery (ssrf) in Azure MCP Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-30223	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.11.1, when JWT authentication is configured using either "authJwtPubKeyPath" (local RSA public key) or "authJwtHmacSecret" (HMAC secret), the configured audience value (authJwtAud) is not enforced during token parsing. As a result, validly signed JWT tokens with an incorrect aud claim are accepted for authentication. This allows authentication using tokens intended for a different audience/service. This issue has been patched in version 3000.11.1.	8.8	More Details
CVE-2026-23654	Dependency on vulnerable third-party component in GitHub Repo: zero-shot-scfoundation allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-27390	Authentication Bypass Using an Alternate Path or Channel vulnerability in designthemes WeDesignTech Ultimate Booking Addon wedesigntech-ultimate-booking-addon allows Authentication Abuse.This issue affects WeDesignTech Ultimate Booking Addon: from n/a through <= 1.0.1.	8.8	More Details
CVE-2026-26416	An authorization bypass vulnerability in Tata Consultancy Services Cognix Recon Client v3.0 allows authenticated users to escalate privileges across role boundaries via crafted requests.	8.8	More Details
CVE-2026-3809	A flaw has been found in Tenda FH1202 1.2.0.14(408). The impacted element is the function fromNatStaticSetting of the file /goform/NatSaticSetting. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-69219	A user with access to the DB could craft a database entry that would result in executing code on Triggerer - which gives anyone who have access to DB the same permissions as Dag Author. Since direct DB access is not usual and recommended for Airflow, the likelihood of it making any damage is low. You should upgrade to version 6.0.0 of the provider to avoid even that risk.	8.8	More Details
CVE-2026-3814	A security flaw has been discovered in UTT HiPER 810G up to 1.7.7-1711. Affected by this issue is the function strcpy of the file /goform/getOneApConfTempEntry. Performing a manipulation results in buffer overflow. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-3811	A vulnerability was found in Tenda FH1202 1.2.0.14(408). This impacts the function fromP2pListFilter of the file /goform/P2pListFilter. The manipulation of the argument page results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-22473	Deserialization of Untrusted Data vulnerability in designthemes Dental Clinic dental allows Object Injection.This issue affects Dental Clinic: from n/a through <= 3.7.	8.8	More Details
CVE-2026-23798	Deserialization of Untrusted Data vulnerability in blubrry PowerPress Podcasting powerpress allows Object Injection.This issue affects PowerPress Podcasting: from n/a through <= 11.15.10.	8.8	More Details
CVE-2026-27338	Deserialization of Untrusted Data vulnerability in AivahThemes Car Zone carzone allows Object Injection.This issue affects Car Zone: from n/a through <= 3.7.	8.8	More Details
CVE-2025-15547	By default, jailed processes cannot mount filesystems, including nullfs(4). However, the allow.mount.nullfs option enables mounting nullfs filesystems, subject to privilege checks. If a privileged user within a jail is able to nullfs-mount directories, a limitation of the kernel's path lookup logic allows that user to escape the jail's chroot, yielding access to the full filesystem of the host or parent jail. In a jail configured to allow nullfs(4) mounts from within the jail, the jailed root user can escape the jail's filesystem root.	8.8	More Details
CVE-2025-41766	A low-privileged remote attacker can trigger a stack-based buffer overflow via a crafted HTTP POST request using the ubr-network method resulting in full device compromise.	8.8	More Details
CVE-2026-3769	A vulnerability was detected in Tenda F453 1.0.0.3. Affected by this issue is the function WrlclientSet of the file /goform/WrlclientSet. The manipulation of the argument GO results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	8.8	More Details
CVE-	A low-privileged remote attacker can exploit an arbitrary file write vulnerability in the wwupload.cgi		

2025-41758	endpoint. Due to path traversal this can lead to overwriting arbitrary files on the device and achieving a full system compromise.	8.8	More Details
CVE-2025-41757	A low-privileged remote attacker can abuse the backup restore functionality of UBR (ubr-restore) which runs with elevated privileges and does not validate the contents of the backup archive to create or overwrite arbitrary files anywhere on the system.	8.8	More Details
CVE-2026-3768	A security vulnerability has been detected in Tenda F453 1.0.0.3. Affected by this vulnerability is the function formWrlExtraSet of the file /goform/WrlExtraSet. The manipulation of the argument GO leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-3288	A security issue was discovered in ingress-nginx where the `nginx.ingress.kubernetes.io/rewrite-target` Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	8.8	More Details
CVE-2026-3810	A vulnerability has been found in Tenda FH1202 1.2.0.14(408). This affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-3799	A flaw has been found in Tenda i3 1.0.0.6(2204). This impacts the function formSetCfm of the file /goform/setcfm. This manipulation of the argument funcpara1 causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-21262	Improper access control in SQL Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-3808	A vulnerability was detected in Tenda FH1202 1.2.0.14(408). The affected element is the function formWebTypeLibrary of the file /goform/webtypelibrary. Performing a manipulation of the argument webSiteId results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-3823	EHG2408 series switch developed by Atop Technologies has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and execute arbitrary code.	8.8	More Details
CVE-2026-27379	Deserialization of Untrusted Data vulnerability in NextScripts NextScripts social-networks-auto-poster-facebook-twitter-g allows Object Injection.This issue affects NextScripts: from n/a through <= 4.4.7.	8.8	More Details
CVE-2026-3807	A security vulnerability has been detected in Tenda FH1202 1.2.0.14(408). Impacted is the function formWrlsafeset of the file /goform/AdvSetWrlsafeset. Such manipulation of the argument mit_ssid/mit_ssid_index leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-3544	Heap buffer overflow in WebCodecs in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-3543	Inappropriate implementation in V8 in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-3542	Inappropriate implementation in WebAssembly in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-3541	Inappropriate implementation in CSS in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-3540	Inappropriate implementation in WebAudio in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-	Object lifecycle issue in DevTools in Google Chrome prior to 145.0.7632.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted	8.8	More

3539	Chrome Extension. (Chromium security severity: High)		Details
CVE-2026-3538	Integer overflow in Skia in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-3537	Object lifecycle issue in PowerVR in Google Chrome on Android prior to 145.0.7632.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-3536	Integer overflow in ANGLE in Google Chrome prior to 145.0.7632.159 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-20967	Improper input validation in System Center Operations Manager allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-29089	TimescaleDB is a time-series database for high-performance real-time analytics packaged as a Postgres extension. From version 2.23.0 to 2.25.1, PostgreSQL uses the search_path setting to locate unqualified database objects (tables, functions, operators). If the search_path includes user-writable schemas a malicious user can create functions in that schema that shadow builtin postgres functions and will be called instead of the postgres functions leading to arbitrary code execution during extension upgrade. This issue has been patched in version 2.25.2.	8.8	More Details
CVE-2026-3701	A security vulnerability has been detected in H3C Magic B1 up to 100R004. Affected by this vulnerability is the function Edit_BasicSSID_5G of the file /goform/aspForm. Such manipulation of the argument param leads to buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-3815	A weakness has been identified in UTT HiPER 810G up to 1.7.7-1711. This affects the function strcpy of the file /goform/formApMail. Executing a manipulation can lead to buffer overflow. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-3047	A flaw was found in org.keycloak.broker.saml. When a disabled Security Assertion Markup Language (SAML) client is configured as an Identity Provider (IdP)-initiated broker landing target, it can still complete the login process and establish a Single Sign-On (SSO) session. This allows a remote attacker to gain unauthorized access to other enabled clients without re-authentication, effectively bypassing security restrictions.	8.8	More Details
CVE-2026-3847	Memory safety bugs present in Firefox 148.0.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 148.0.2.	8.8	More Details
CVE-2026-3845	Heap buffer overflow in the Audio/Video: Playback component in Firefox for Android. This vulnerability affects Firefox < 148.0.2.	8.8	More Details
CVE-2026-29073	SiYuan is a personal knowledge management system. Prior to version 3.6.0, the /api/query/sql lets a user run sql directly, but it only checks basic auth, not admin rights, any logged-in user, even readers, can run any sql query on the database. This issue has been patched in version 3.6.0.	8.8	More Details
CVE-2026-29610	OpenClaw versions prior to 2026.2.14 contain a command hijacking vulnerability that allows attackers to execute unintended binaries by manipulating PATH environment variables through node-host execution or project-local bootstrapping. Attackers with authenticated access to node-host execution surfaces or those running OpenClaw in attacker-controlled directories can place malicious executables in PATH to override allowlisted safe-bin commands and achieve arbitrary command execution.	8.8	More Details
CVE-2025-70995	An issue in Aranda Service Desk Web Edition (ASDK API 8.6) allows authenticated attackers to achieve remote code execution due to improper validation of uploaded files. An authenticated user can upload a crafted web.config file by sending a crafted POST request to /ASDKAPI/api/v8.6/item/addfile, which is processed by the ASP.NET runtime. The uploaded configuration file alters the execution context of the upload directory, enabling compilation and execution of attacker-controlled code (e.g., generation of an .aspx webshell). This allows remote command execution on the server without user interaction beyond authentication, impacting both On-Premise and SaaS deployments.	8.8	More Details
	An OS Command Injection vulnerability exists in the web-based Traceroute diagnostic utility of		

CVE-2026-28774	International Datacasting Corporation (IDC) SFX Series SuperFlex SatelliteReceiver Web Management Interface version 101. An authenticated attacker can inject arbitrary shell metacharacters (such as the pipe `|` operator) into the flags parameter, leading to the execution of arbitrary operating system commands with root privileges.	8.8	More Details
CVE-2026-28770	Improper neutralization of special elements in the /IDC_Logging/checkifdone.cgi script in International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver Web management Interface version 101 allows for XML Injection. The application reflects un-sanitized user input from the `file` parameter directly into a CDATA block, allowing an authenticated attacker to break out of the tags and inject arbitrary XML elements. An actor is confirmed to be able to turn this into an reflected XSS but further abuse such as XXE may be possible	8.8	More Details
CVE-2026-28676	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Prior to version 1.6.3-alpha, multiple storage helpers used path construction patterns that did not uniformly enforce base-directory containment. This created path-injection risk in file read/write/delete flows if malicious path-like values were introduced. This issue has been patched in version 1.6.3-alpha.	8.8	More Details
CVE-2025-15602	Snipe-IT versions prior to 8.3.7 contain sensitive user attributes related to account privileges that are insufficiently protected against mass assignment. An authenticated, low-privileged user can craft a malicious API request to modify restricted fields of another user account, including the Super Admin account. By changing the email address of the Super Admin and triggering a password reset, an attacker can fully take over the Super Admin account, resulting in complete administrative control of the Snipe-IT instance.	8.8	More Details
CVE-2026-30944	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.0, the /studiocms_api/dashboard/api-tokens endpoint allows any authenticated user (at least Editor) to generate API tokens for any other user, including owner and admin accounts. The endpoint fails to validate whether the requesting user is authorized to create tokens on behalf of the target user ID, resulting in a full privilege escalation. This vulnerability is fixed in 0.4.0.	8.8	More Details
CVE-2026-28773	The web-based Ping diagnostic utility (/IDC_Ping/main.cgi) in International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver Web Management Interface version 101 is vulnerable to OS Command Injection. The application insecurely parses the `IPaddr` parameter. An authenticated attacker can bypass server-side semicolon exclusion checks by using alternate shell metacharacters (such as the pipe `|` operator) to append and execute arbitrary shell commands with root privileges.	8.8	More Details
CVE-2026-25888	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.1, there is a remote code execution vulnerability via a vulnerable API. This issue has been patched in version 4.8.1.	8.8	More Details
CVE-2026-28287	FreePBX is an open source IP PBX. From versions 16.0.17.2 to before 16.0.20 and from version 17.0.2.4 to before 17.0.5, multiple command injection vulnerabilities exist in the recordings module. This issue has been patched in versions 16.0.20 and 17.0.5.	8.8	More Details
CVE-2025-55289	Chamilo is a learning management system. Prior to version 1.11.34, there is a stored XSS vulnerability in Chamilo LMS (Verison 1.11.32) allows an attacker to inject arbitrary JavaScript into the platform’s social network and internal messaging features. When viewed by an authenticated user (including administrators), the payload executes in their browser within the LMS context. This enables full account takeover via session hijacking, unauthorized actions with the victim’s privileges, exfiltration of sensitive data, and potential self-propagation to other users. This issue has been patched in version 1.11.34.	8.8	More Details
CVE-2026-28210	FreePBX is an open source IP PBX. Prior to versions 16.0.49 and 17.0.7, FreePBX module cdr (Call Data Record) is vulnerable to SQL query injection. This issue has been patched in versions 16.0.49 and 17.0.7.	8.8	More Details
CVE-2026-28284	FreePBX is an open source IP PBX. Prior to versions 16.0.10 and 17.0.5, the FreePBX logfiles module contains several authenticated SQL injection vulnerabilities. This issue has been patched in versions 16.0.10 and 17.0.5.	8.8	More Details
CVE-2026-29041	Chamilo is a learning management system. Prior to version 1.11.34, Chamilo LMS is affected by an authenticated remote code execution vulnerability caused by improper validation of uploaded files. The application relies solely on MIME-type verification when handling file uploads and does not adequately validate file extensions or enforce safe server-side storage restrictions. As a result, an authenticated low-privileged user can upload a crafted file containing executable code and subsequently execute arbitrary commands on the server. This issue has been patched in version 1.11.34.	8.8	More Details
CVE-	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, a stored cross-site scripting		

2026-26022	(XSS) vulnerability exists in the comment and issue description functionality. The application's HTML sanitizer explicitly allows data: URI schemes, enabling authenticated users to inject arbitrary JavaScript execution via malicious links. This issue has been patched in version 0.14.2.	8.7	More Details
CVE-2026-28683	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to version 2.2.3, if a malicious authenticated user uploads SVG and creates a hotlink for it, they can achieve stored XSS. This issue has been patched in version 2.2.3.	8.7	More Details
CVE-2026-20101	A vulnerability in the SAML 2.0 single sign-on (SSO) feature of Cisco Secure Firewall ASA Software and Secure FTD Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability is due to insufficient error checking when processing SAML messages. An attacker could exploit this vulnerability by sending crafted SAML messages to the SAML service. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2026-21333	Illustrator versions 29.8.4, 30.1 and earlier are affected by an Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.6	More Details
CVE-2026-20103	A vulnerability in the Remote Access SSL VPN functionality of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to exhaust device memory resulting in a denial of service (DoS) condition to new Remote Access SSL VPN connections. This does not affect the management interface, though it may become temporarily unresponsive. This vulnerability is due to trusting user input without validation. An attacker could exploit this vulnerability by sending crafted packets to the Remote Access SSL VPN server. A successful exploit could allow the attacker to cause the device web interface to stop responding, resulting in a DoS condition.	8.6	More Details
CVE-2026-28679	Home-Gallery.org is a self-hosted open-source web gallery to browse personal photos and videos. Prior to version 1.21.0, when a user requests a download, the application does not verify whether the requested file is located within the media source directory, which can result in sensitive system files being downloadable as well. This issue has been patched in version 1.21.0.	8.6	More Details
CVE-2026-26125	Payment Orchestrator Service Elevation of Privilege Vulnerability	8.6	More Details
CVE-2026-22471	Deserialization of Untrusted Data vulnerability in maximsecudeal Secudeal Payments for Ecommerce secudeal-payments-for-ecommerce allows Object Injection.This issue affects Secudeal Payments for Ecommerce: from n/a through <= 1.1.	8.6	More Details
CVE-2026-20039	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to ineffective memory management of the VPN web server. An attacker could exploit this vulnerability by sending a large number of&nbsp;crafted HTTP requests to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2026-30920	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.19, OneUptime's GitHub App callback trusts attacker-controlled state and installation_id values and updates Project.gitHubAppInstallationId with isRoot: true without validating that the caller is authorized for the target project. This allows an attacker to overwrite another project's GitHub App installation binding. Related GitHub endpoints also lack effective authorization, so a valid installation ID can be used to enumerate repositories and create CodeRepository records in an arbitrary project. This vulnerability is fixed in 10.0.19.	8.6	More Details
CVE-2026-20082	A vulnerability in the handling of the embryonic connection limits in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause incoming TCP SYN packets to be dropped incorrectly. This vulnerability is due to improper handling of new, incoming TCP connections that are destined to management or data interfaces when the device is under a TCP SYN flood attack. An attacker could exploit this vulnerability by sending a crafted stream of traffic to an affected device. A successful exploit could allow the attacker to prevent all incoming TCP connections to the device from being established, including remote management access, Remote Access VPN (RAVPN) connections, and all network protocols that are TCP-based. This results in a denial of service (DoS) condition for affected features.	8.6	More Details
CVE-2026-22460	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in wpWax FormGent formgent allows Path Traversal.This issue affects FormGent: from n/a through <= 1.4.2.	8.6	More Details

CVE-2026-31817	OliveTin gives access to predefined shell commands from a web interface. Prior to 3000.11.2, when the saveLogs feature is enabled, OliveTin persists execution log entries to disk. The filename used for these log files is constructed in part from the user-supplied UniqueTrackingId field in the StartAction API request. This value is not validated or sanitized before being used in a file path, allowing an attacker to use directory traversal sequences (e.g., ../../../) to write files to arbitrary locations on the filesystem. This vulnerability is fixed in 3000.11.2.	8.5	More Details
CVE-2026-30242	Plane is an an open-source project management tool. Prior to version 1.2.3, the webhook URL validation in plane/app/serializers/webhook.py only checks ip.is_loopback, allowing attackers with workspace ADMIN role to create webhooks pointing to private/internal network addresses (10.x.x.x, 172.16.x.x, 192.168.x.x, 169.254.169.254, etc.). When webhook events fire, the server makes requests to these internal addresses and stores the response — enabling SSRF with full response read-back. This issue has been patched in version 1.2.3.	8.5	More Details
CVE-2026-27373	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Essekia Tablesome tablesome allows Blind SQL Injection.This issue affects Tablesome: from n/a through <= 1.2.3.	8.5	More Details
CVE-2026-28513	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to your services. Prior to 2.4.0, the OIDC token endpoint rejects an authorization code only when both the client ID is wrong and the code is expired. This allows cross-client code exchange and expired code reuse. This vulnerability is fixed in 2.4.0.	8.5	More Details
CVE-2026-28134	Improper Control of Generation of Code ('Code Injection') vulnerability in Crocoblock JetEngine jet-engine allows Remote Code Inclusion.This issue affects JetEngine: from n/a through <= 3.7.2.	8.5	More Details
CVE-2026-27428	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eagle-Themes Eagle Booking eagle-booking allows SQL Injection.This issue affects Eagle Booking: from n/a through <= 1.3.4.3.	8.5	More Details
CVE-2026-28442	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.5.2-beta3, users are restricted from deleting internal system files or folders through the application interface. However, when interacting directly with the API, these restrictions can be bypassed. By altering the path parameter in the delete request, internal OS files and directories can be removed successfully. The backend processes these manipulated requests without validating whether the targeted path belongs to restricted system locations. This demonstrates improper input validation and broken access control on sensitive filesystem operations. No known public patch is available.	8.5	More Details
CVE-2026-26109	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-28463	OpenClaw exec-approvals allowlist validation checks pre-expansion argv tokens but execution uses real shell expansion, allowing safe bins like head, tail, or grep to read arbitrary local files via glob patterns or environment variables. Authorized callers or prompt-injection attacks can exploit this to disclose files readable by the gateway or node process when host execution is enabled in allowlist mode.	8.4	More Details
CVE-2026-26113	Untrusted pointer dereference in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-26110	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-28485	OpenClaw versions 2026.1.5 prior to 2026.2.12 fail to enforce mandatory authentication on the /agent/act browser-control HTTP route, allowing unauthorized local callers to invoke privileged operations. Remote attackers on the local network or local processes can execute arbitrary browser-context actions and access sensitive in-session data by sending requests to unauthenticated endpoints.	8.4	More Details
CVE-2026-0122	In multiple places, there is a possible out of bounds write due to memory corruption. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-	In EfwApTransport::ProcessRxRing of efw_ap_transport.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution	8.4	More

0123	privileges needed. User interaction is not needed for exploitation.		Details
CVE-2026-28476	OpenClaw versions prior to 2026.2.14 contain a server-side request forgery vulnerability in the optional Tlon Urbit extension that accepts user-provided base URLs for authentication without proper validation. Attackers who can influence the configured Urbit URL can induce the gateway to make HTTP requests to arbitrary hosts including internal addresses.	8.3	More Details
CVE-2026-28451	OpenClaw versions prior to 2026.2.14 contain server-side request forgery vulnerabilities in the Feishu extension that allow attackers to fetch attacker-controlled remote URLs without SSRF protections via sendMediaFeishu function and markdown image processing. Attackers can influence tool calls through direct manipulation or prompt injection to trigger requests to internal services and re-upload responses as Feishu media.	8.3	More Details
CVE-2026-29075	Mesa is an open-source Python library for agent-based modeling, simulating complex systems and exploring emergent behaviors. In version 3.5.0 and prior, checking out of untrusted code in benchmarks.yml workflow may lead to code execution in privileged runner. This issue has been patched via commit c35b8cd.	8.3	More Details
CVE-2026-27802	Vaultwarden is an unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. Prior to version 1.35.4, there is a privilege escalation vulnerability via bulk permission update to unauthorized collections by Manager. This issue has been patched in version 1.35.4.	8.3	More Details
CVE-2026-27803	Vaultwarden is an unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. Prior to version 1.35.4, when a Manager has manage=false for a given collection, they can still perform several management operations as long as they have access to the collection. This issue has been patched in version 1.35.4.	8.3	More Details
CVE-2018-25163	BitZoom 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the rollno and username parameters in forgot.php and login.php. Attackers can submit crafted POST requests with SQL UNION statements to extract database schema information and table contents from the application database.	8.2	More Details
CVE-2026-28787	OneUptime is a solution for monitoring and managing online services. In version 10.0.11 and prior, the WebAuthn authentication implementation does not store the challenge on the server side. Instead, the challenge is returned to the client and accepted back from the client request body during verification. This violates the WebAuthn specification (W3C Web Authentication Level 2, §13.4.3) and allows an attacker who has obtained a valid WebAuthn assertion (e.g., via XSS, MitM, or log exposure) to replay it indefinitely, completely bypassing the second-factor authentication. No known patches are available.	8.2	More Details
CVE-2026-28677	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Prior to version 1.6.3-alpha, the URL ingest pipeline accepted user-controlled remote URLs with incomplete destination restrictions. Although private/local host checks existed, missing restrictions for credentialed URLs, non-standard ports, and cross-host redirects left SSRF-class abuse paths in non-localhost deployments. This issue has been patched in version 1.6.3-alpha.	8.2	More Details
CVE-2018-25176	Alive Parish 2.0.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the key parameter in the search endpoint. Attackers can also upload arbitrary files via the person photo upload functionality to the images/uploaded directory for remote code execution.	8.2	More Details
CVE-2018-25175	Alienor Web Libre 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the identifiant parameter. Attackers can submit crafted POST requests to index.php with SQL injection payloads in the identifiant field to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2026-27826	MCP Atlassian is a Model Context Protocol (MCP) server for Atlassian products (Confluence and Jira). Prior to version 0.17.0, an unauthenticated attacker who can reach the mcp-atlassian HTTP endpoint can force the server process to make outbound HTTP requests to an arbitrary attacker-controlled URL by supplying two custom HTTP headers without an `Authorization` header. No authentication is required. The vulnerability exists in the HTTP middleware and dependency injection layer — not in any MCP tool handler - making it invisible to tool-level code analysis. In cloud deployments, this could enable theft of IAM role credentials via the instance metadata endpoint (`169[.]254[.]169[.]254`). In any HTTP deployment it enables internal network reconnaissance and injection of attacker-controlled content into LLM tool results. Version 0.17.0 fixes the issue.	8.2	More Details
CVE-2018-25172	Pedidos 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'q' parameter. Attackers can send GET requests to the ajax/load_proveedores.php endpoint with crafted SQL payloads to extract sensitive database information including schema names and table structures.	8.2	More Details

CVE-2018-25173	Rmedia SMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through the gid parameter. Attackers can send GET requests to editgrp.php with malicious gid values using EXTRACTVALUE and CONCAT functions to retrieve schema names and sensitive database data.	8.2	More Details
CVE-2018-25166	Meneame English Pligg 5.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the search parameter. Attackers can send GET requests to index.php with crafted SQL payloads in the search parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25171	EdTv 2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to the admin/edit_source endpoint with crafted SQL UNION statements to extract database information including schema names, user credentials, and version details.	8.2	More Details
CVE-2018-25167	Net-Billetterie 2.9 contains an SQL injection vulnerability in the login parameter of login.inc.php that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can submit malicious SQL code through the login POST parameter to extract database information including usernames, passwords, and system credentials.	8.2	More Details
CVE-2026-31824	Sylius is an Open Source eCommerce Framework on Symfony. A Time-of-Check To Time-of-Use (TOCTOU) race condition was discovered in the promotion usage limit enforcement. The same class of vulnerability affects the promotion usage limit (the global used counter on Promotion entities), coupon usage limit (the global used counter on PromotionCoupon entities), and coupon per-customer usage limit (the per-customer redemption count on PromotionCoupon entities). In all three cases, the eligibility check reads the used counter (or order count) from an in-memory Doctrine entity during validation, while the actual usage increment in OrderPromotionsUsageModifier happens later during order completion — with no database-level locking or atomic operations between the two phases. Because Doctrine flushes an absolute value (SET used = 1) rather than an atomic increment (SET used = used + 1), and because the affected entities lack optimistic locking, concurrent requests all read the same stale usage counts and pass the eligibility checks simultaneously. An attacker can exploit this by preparing multiple carts with the same limited-use promotion or coupon and firing simultaneous PATCH /api/v2/shop/orders/{token}/complete requests. All requests pass the usage limit checks and complete successfully, allowing a single-use promotion or coupon to be redeemed an arbitrary number of times. The per-customer limit can be bypassed in the same way by a single customer completing multiple orders concurrently. No authentication is required to exploit this vulnerability. This may lead to direct financial loss through unlimited redemption of limited-use promotions and discount coupons. The issue is fixed in versions: 1.9.12, 1.10.16, 1.11.17, 1.12.23, 1.13.15, 1.14.18, 2.0.16, 2.1.12, 2.2.3 and above.	8.2	More Details
CVE-2018-25161	Warranty Tracking System 11.06.3 contains an SQL injection vulnerability that allows attackers to execute arbitrary SQL queries by injecting malicious code through the txtCustomerCode, txtCustomerName, and txtPhone POST parameters in SearchCustomer.php. Attackers can submit crafted SQL statements using UNION SELECT to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2026-29064	Zarf is an Airgap Native Packager Manager for Kubernetes. From version 0.54.0 to before version 0.73.1, a path traversal vulnerability in archive extraction allows a specifically crafted Zarf package to create symlinks pointing outside the destination directory, enabling arbitrary file read or write on the system processing the package. This issue has been patched in version 0.73.1.	8.2	More Details
CVE-2018-25170	DoceboLMS 1.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the id, idC, and idU parameters. Attackers can send GET requests to the lesson.php endpoint with malicious SQL payloads to extract sensitive database information.	8.2	More Details
CVE-2018-25188	Webiness Inventory 2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the order parameter. Attackers can send POST requests to the WsModelGrid.php endpoint with crafted SQL payloads to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2019-25498	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the landing_location parameter. Attackers can send POST requests to the searched endpoint with malicious SQL payloads to bypass authentication and extract sensitive database information.	8.2	More Details
CVE-	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the job_id parameter. Attackers can send		More

2019-25499	POST requests to get_job_applications_ajax.php with malicious job_id values to bypass authentication, extract sensitive data, or modify database contents.	8.2	Details
CVE-2019-25500	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the employerid parameter. Attackers can send POST requests to the register-recruiters endpoint with time-based SQL injection payloads to extract sensitive data or modify database contents.	8.2	More Details
CVE-2019-25501	Simple Job Script contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting malicious SQL code through the app_id parameter. Attackers can send POST requests to delete_application_ajax.php with crafted payloads to extract sensitive data, bypass authentication, or modify database contents.	8.2	More Details
CVE-2019-25504	NCrypted Jobgator contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the experience parameter. Attackers can send POST requests to the agents Find-Jobs endpoint with malicious experience values to extract sensitive database information.	8.2	More Details
CVE-2019-25506	FreeSMS 2.1.2 contains a boolean-based blind SQL injection vulnerability in the password parameter that allows unauthenticated attackers to bypass authentication by injecting SQL code through the login endpoint. Attackers can exploit the vulnerable password parameter in requests to /pages/crc_handler.php?method=login to authenticate as any known user and subsequently modify their password via the profile update function.	8.2	More Details
CVE-2019-25507	Ashop Shopping Cart Software contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'shop' parameter. Attackers can send GET requests to index.php with malicious 'shop' values using UNION-based SQL injection to extract sensitive database information.	8.2	More Details
CVE-2026-29193	ZITADEL is an open source identity management platform. From version 4.0.0 to 4.12.0, a vulnerability in Zitadel's login V2 UI allowed users to bypass login behavior and security policies and self-register new accounts or sign in using password even if corresponding options were disabled in their organizaton. This issue has been patched in version 4.12.1.	8.2	More Details
CVE-2018-25199	OOP CMS BLOG 1.0 contains SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through multiple parameters. Attackers can inject SQL commands via the search parameter in search.php, pageid parameter in page.php, and id parameter in posts.php to extract database information including table names, schema names, and database credentials.	8.2	More Details
CVE-2018-25196	ServerZilla 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the email parameter. Attackers can send POST requests to reset.php with malicious email values containing SQL operators to bypass authentication and extract sensitive database information.	8.2	More Details
CVE-2018-25194	Nominas 0.27 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the username parameter. Attackers can send POST requests to the login/checklogin.php endpoint with crafted UNION-based SQL injection payloads to extract database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25192	GPS Tracking System 2.12 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can submit crafted POST requests to the login.php endpoint with SQL injection payloads in the username field to gain unauthorized access without valid credentials.	8.2	More Details
CVE-2018-25189	Data Center Audit 2.6.2 contains an SQL injection vulnerability in the username parameter of dca_login.php that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can submit crafted SQL payloads through POST requests to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25197	PlayJoom 0.10.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the catid parameter. Attackers can send GET requests to index.php with option=com_playjoom&view=genre&catid=[SQL] to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2026-28135	Inclusion of Functionality from Untrusted Control Sphere vulnerability in WP Royal Royal Elementor Addons royal-elementor-addons allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Royal Elementor Addons: from n/a through <= 1.7.1049.	8.2	More Details

CVE-2018-25179	Gumbo CMS 0.99 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the language parameter. Attackers can send POST requests to the settings endpoint with crafted SQL payloads in the language parameter to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2018-25182	Silurus Classifieds Script 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the ID parameter. Attackers can send GET requests to wcategory.php with crafted SQL payloads in the ID parameter to extract database table names and sensitive information from the database.	8.2	More Details
CVE-2018-25187	Tina4 Stack 1.0.3 contains multiple vulnerabilities allowing unauthenticated attackers to access sensitive database files and execute SQL injection attacks. Attackers can directly request the kim.db database file to retrieve user credentials and password hashes, or inject SQL code through the menu endpoint to manipulate database queries.	8.2	More Details
CVE-2026-28016	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Luxury Wine luxury-wine allows PHP Local File Inclusion.This issue affects Luxury Wine: from n/a through <= 1.1.14.	8.1	More Details
CVE-2026-22441	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Zentrum zentrum allows PHP Local File Inclusion.This issue affects Zentrum: from n/a through <= 1.0.	8.1	More Details
CVE-2026-28051	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Yacht Rental yacht-rental allows PHP Local File Inclusion.This issue affects Yacht Rental: from n/a through <= 2.6.	8.1	More Details
CVE-2026-28050	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Beacon beacon allows PHP Local File Inclusion.This issue affects Beacon: from n/a through <= 2.24.	8.1	More Details
CVE-2026-22442	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in LaunchandSell Tribe tribe allows PHP Local File Inclusion.This issue affects Tribe: from n/a through <= 1.7.3.	8.1	More Details
CVE-2026-27097	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes CasaMia | Property Rental Real Estate WordPress Theme casamia allows PHP Local File Inclusion.This issue affects CasaMia | Property Rental Real Estate WordPress Theme: from n/a through <= 1.1.2.	8.1	More Details
CVE-2026-28017	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Green Thumb greenthumb allows PHP Local File Inclusion.This issue affects Green Thumb: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-27098	Deserialization of Untrusted Data vulnerability in axiomthemes Au Pair Agency - Babysitting & Nanny Theme au-pair-agency allows Object Injection.This issue affects Au Pair Agency - Babysitting & Nanny Theme: from n/a through <= 1.2.2.	8.1	More Details
CVE-2026-27326	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes AC Services | HVAC, Air Conditioning & Heating Company WordPress Theme window-ac-services allows PHP Local File Inclusion.This issue affects AC Services | HVAC, Air Conditioning & Heating Company WordPress Theme: from n/a through <= 1.2.5.	8.1	More Details
CVE-2026-28049	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Police Department police-department allows PHP Local File Inclusion.This issue affects Police Department: from n/a through <= 2.17.	8.1	More Details
CVE-2026-27337	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Chronicle - Lifestyle Magazine & Blog WordPress Theme chronicle allows PHP Local File Inclusion.This issue affects Chronicle - Lifestyle Magazine & Blog WordPress Theme: from n/a through <= 1.0.	8.1	More Details
CVE-2026-28014	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Translogic translogic allows PHP Local File Inclusion.This issue affects Translogic: from n/a through <= 1.2.11.	8.1	More Details
CVE-2026-22446	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Prowess prowess allows PHP Local File Inclusion.This issue affects Prowess: from n/a through <= 1.8.1.	8.1	More Details

CVE-2026-27334	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in dan_fisher Alchemists alchemists allows PHP Local File Inclusion.This issue affects Alchemists: from n/a through <= 4.6.0.	8.1	More Details
CVE-2026-27335	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Ekoterra - NonProfit, Green Energy & Ecology Theme ekoterra allows PHP Local File Inclusion.This issue affects Ekoterra - NonProfit, Green Energy & Ecology Theme: from n/a through <= 1.0.0.	8.1	More Details
CVE-2026-22439	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Green Planet green-planet allows PHP Local File Inclusion.This issue affects Green Planet: from n/a through <= 1.1.14.	8.1	More Details
CVE-2026-28048	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in magentech FlashMart flashmart allows PHP Local File Inclusion.This issue affects FlashMart: from n/a through <= 2.0.15.	8.1	More Details
CVE-2026-27336	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Consultor | Consulting, Accounting & Legal Counsel WordPress Theme consultor allows PHP Local File Inclusion.This issue affects Consultor | Consulting, Accounting & Legal Counsel WordPress Theme: from n/a through <= 1.2.4.	8.1	More Details
CVE-2026-22443	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Alliance alliance allows PHP Local File Inclusion.This issue affects Alliance: from n/a through <= 3.1.1.	8.1	More Details
CVE-2026-23801	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes The Issue theissue allows PHP Local File Inclusion.This issue affects The Issue: from n/a through <= 1.6.11.	8.1	More Details
CVE-2026-22456	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Askka askka allows PHP Local File Inclusion.This issue affects Askka: from n/a through <= 1.0.	8.1	More Details
CVE-2026-22449	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Don Peppe donpeppe allows PHP Local File Inclusion.This issue affects Don Peppe: from n/a through <= 1.3.	8.1	More Details
CVE-2026-22457	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Wanderland wanderland allows PHP Local File Inclusion.This issue affects Wanderland: from n/a through <= 1.5.	8.1	More Details
CVE-2026-28013	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Kratz kratz allows PHP Local File Inclusion.This issue affects Kratz: from n/a through <= 1.0.12.	8.1	More Details
CVE-2026-28012	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Gridiron gridiron allows PHP Local File Inclusion.This issue affects Gridiron: from n/a through <= 1.0.14.	8.1	More Details
CVE-2026-28056	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX MCKinney's Politics mckinney-politics allows PHP Local File Inclusion.This issue affects MCKinney's Politics: from n/a through <= 1.2.8.	8.1	More Details
CVE-2026-28055	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX M.Williamson williamson allows PHP Local File Inclusion.This issue affects M.Williamson: from n/a through <= 1.2.11.	8.1	More Details
CVE-2026-28011	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Yottis yottis allows PHP Local File Inclusion.This issue affects Yottis: from n/a through <= 1.0.10.	8.1	More Details
CVE-2026-28015	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX ShiftCV shift-cv allows PHP Local File Inclusion.This issue affects ShiftCV: from n/a through <= 3.0.14.	8.1	More Details
CVE-2026-28027	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Kayon kayon allows PHP Local File Inclusion.This issue affects Kayon: from n/a through <= 1.3.	8.1	More Details

CVE-2026-22452	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Hoverex hoverex allows PHP Local File Inclusion.This issue affects Hoverex: from n/a through <= 1.5.10.	8.1	More Details
CVE-2026-22476	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Etchy etchy allows PHP Local File Inclusion.This issue affects Etchy: from n/a through <= 1.0.	8.1	More Details
CVE-2026-22477	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Felizia felizia allows PHP Local File Inclusion.This issue affects Felizia: from n/a through <= 1.3.4.	8.1	More Details
CVE-2026-27341	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes TopScorer - Sports WordPress Theme topscorer allows PHP Local File Inclusion.This issue affects TopScorer - Sports WordPress Theme: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22478	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes FindAll findall allows PHP Local File Inclusion.This issue affects FindAll: from n/a through <= 1.4.	8.1	More Details
CVE-2026-28054	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Legal Stone legal-stone allows PHP Local File Inclusion.This issue affects Legal Stone: from n/a through <= 1.2.11.	8.1	More Details
CVE-2026-28053	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Miller christine-miller allows PHP Local File Inclusion.This issue affects Miller: from n/a through <= 1.3.3.	8.1	More Details
CVE-2026-28026	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Motorix motorix allows PHP Local File Inclusion.This issue affects Motorix: from n/a through <= 1.6.	8.1	More Details
CVE-2026-28052	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Peter Mason petermason allows PHP Local File Inclusion.This issue affects Peter Mason: from n/a through <= 1.4.5.	8.1	More Details
CVE-2026-27340	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Apollo | Night Club, DJ Event WordPress Theme apollo allows PHP Local File Inclusion.This issue affects Apollo | Night Club, DJ Event WordPress Theme: from n/a through <= 1.3.1.	8.1	More Details
CVE-2026-27989	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Quanzo quanzo allows PHP Local File Inclusion.This issue affects Quanzo: from n/a through <= 1.0.10.	8.1	More Details
CVE-2026-27342	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes TopFit - Fitness and Gym WordPress Theme topfit allows PHP Local File Inclusion.This issue affects TopFit - Fitness and Gym WordPress Theme: from n/a through <= 1.9.	8.1	More Details
CVE-2026-28019	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Manoir manoir allows PHP Local File Inclusion.This issue affects Manoir: from n/a through <= 1.11.	8.1	More Details
CVE-2026-22437	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Playa playa allows PHP Local File Inclusion.This issue affects Playa: from n/a through <= 1.3.9.	8.1	More Details
CVE-2026-28024	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Helion helion allows PHP Local File Inclusion.This issue affects Helion: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-28023	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Nuts nuts allows PHP Local File Inclusion.This issue affects Nuts: from n/a through <= 1.10.	8.1	More Details
CVE-2026-28033	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Edifice edifice allows PHP Local File Inclusion.This issue affects Edifice: from n/a through <= 1.8.	8.1	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File		

2026-28032	Inclusion') vulnerability in ThemeREX Tuning tuning allows PHP Local File Inclusion.This issue affects Tuning: from n/a through <= 1.3.	8.1	More Details
CVE-2026-27994	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Tediss tediss allows PHP Local File Inclusion.This issue affects Tediss: from n/a through <= 1.2.4.	8.1	More Details
CVE-2026-27993	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Aldo aldo allows PHP Local File Inclusion.This issue affects Aldo: from n/a through <= 1.0.10.	8.1	More Details
CVE-2026-28031	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Invetex invetex allows PHP Local File Inclusion.This issue affects Invetex: from n/a through <= 2.18.	8.1	More Details
CVE-2026-28030	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Bonbon bonbon allows PHP Local File Inclusion.This issue affects Bonbon: from n/a through <= 1.6.	8.1	More Details
CVE-2026-28022	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Foodie foodie allows PHP Local File Inclusion.This issue affects Foodie: from n/a through <= 1.14.	8.1	More Details
CVE-2026-27992	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Meals & Wheels meals-wheels allows PHP Local File Inclusion.This issue affects Meals & Wheels: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-27991	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Avventure avventure allows PHP Local File Inclusion.This issue affects Avventure: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-27985	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Humanum humanum allows PHP Local File Inclusion.This issue affects Humanum: from n/a through <= 1.1.4.	8.1	More Details
CVE-2026-27986	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX OsTende ostende allows PHP Local File Inclusion.This issue affects OsTende: from n/a through <= 1.4.3.	8.1	More Details
CVE-2026-28021	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Craftis craftis allows PHP Local File Inclusion.This issue affects Craftis: from n/a through <= 1.2.8.	8.1	More Details
CVE-2026-27990	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX ConFix confix allows PHP Local File Inclusion.This issue affects ConFix: from n/a through <= 1.013.	8.1	More Details
CVE-2026-27987	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX The Qlean the-qlean allows PHP Local File Inclusion.This issue affects The Qlean: from n/a through <= 2.12.	8.1	More Details
CVE-2026-28020	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Chroma chroma allows PHP Local File Inclusion.This issue affects Chroma: from n/a through <= 1.11.	8.1	More Details
CVE-2026-28034	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Progress progress allows PHP Local File Inclusion.This issue affects Progress: from n/a through <= 1.2.	8.1	More Details
CVE-2026-28047	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in magentech Victo victo allows PHP Local File Inclusion.This issue affects Victo: from n/a through <= 1.4.16.	8.1	More Details
CVE-2026-27383	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RadiusTheme Metro metro allows PHP Local File Inclusion.This issue affects Metro: from n/a through <= 2.13.	8.1	More Details
CVE-2026-28046	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Law Office law-office allows PHP Local File Inclusion.This issue affects Law Office: from n/a through <= 3.3.0.	8.1	More Details

CVE-2026-28045	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX N7 | Golf Club Sports & Events n7-golf-club allows PHP Local File Inclusion.This issue affects N7 | Golf Club Sports & Events: from n/a through <= 2.16.0.	8.1	More Details
CVE-2026-28010	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Scientia scientia allows PHP Local File Inclusion.This issue affects Scientia: from n/a through <= 1.2.4.	8.1	More Details
CVE-2026-28009	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX DroneX dronex allows PHP Local File Inclusion.This issue affects DroneX: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-28007	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Coinpress coinpress allows PHP Local File Inclusion.This issue affects Coinpress: from n/a through <= 1.0.14.	8.1	More Details
CVE-2026-27988	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Equadio equadio allows PHP Local File Inclusion.This issue affects Equadio: from n/a through <= 1.1.3.	8.1	More Details
CVE-2025-41756	A low-privileged remote attacker can exploit the ubr-editfile method in wwwubr.cgi, an undocumented and unused API endpoint to write arbitrary files on the system.	8.1	More Details
CVE-2026-28025	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Stargaze stargaze allows PHP Local File Inclusion.This issue affects Stargaze: from n/a through <= 1.5.	8.1	More Details
CVE-2026-28006	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Yungen yungen allows PHP Local File Inclusion.This issue affects Yungen: from n/a through <= 1.0.12.	8.1	More Details
CVE-2026-27369	Deserialization of Untrusted Data vulnerability in BoldThemes Celeste celeste allows Object Injection.This issue affects Celeste: from n/a through <= 1.3.6.	8.1	More Details
CVE-2026-28018	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Global Logistics globallogistics allows PHP Local File Inclusion.This issue affects Global Logistics: from n/a through <= 3.20.	8.1	More Details
CVE-2026-27998	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Vixus vixus allows PHP Local File Inclusion.This issue affects Vixus: from n/a through <= 1.0.16.	8.1	More Details
CVE-2026-28035	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Printy printy allows PHP Local File Inclusion.This issue affects Printy: from n/a through <= 1.8.	8.1	More Details
CVE-2026-27997	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Maxify maxify allows PHP Local File Inclusion.This issue affects Maxify: from n/a through <= 1.0.16.	8.1	More Details
CVE-2026-27996	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Lingvico lingvico allows PHP Local File Inclusion.This issue affects Lingvico: from n/a through <= 1.0.14.	8.1	More Details
CVE-2026-27995	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Justitia justitia allows PHP Local File Inclusion.This issue affects Justitia: from n/a through <= 1.1.0.	8.1	More Details
CVE-2026-27381	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Aora aora allows PHP Local File Inclusion.This issue affects Aora: from n/a through <= 1.3.15.	8.1	More Details
CVE-2026-28041	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Grit grit allows PHP Local File Inclusion.This issue affects Grit: from n/a through <= 1.0.1.	8.1	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File		

2026- 28089	Inclusion') vulnerability in ThemeREX Daiquiri daiquiri allows PHP Local File Inclusion.This issue affects Daiquiri: from n/a through <= 1.2.4.	8.1	More Details
CVE- 2026- 22436	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Helvig helvig allows PHP Local File Inclusion.This issue affects Helvig: from n/a through <= 1.0.	8.1	More Details
CVE- 2026- 28094	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX RexCoin rexcoin allows PHP Local File Inclusion.This issue affects RexCoin: from n/a through <= 1.2.6.	8.1	More Details
CVE- 2026- 28121	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Anderson andersonclinic allows PHP Local File Inclusion.This issue affects Anderson: from n/a through <= 1.4.2.	8.1	More Details
CVE- 2026- 28120	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Dr.Patterson dr-patterson allows PHP Local File Inclusion.This issue affects Dr.Patterson: from n/a through <= 1.3.2.	8.1	More Details
CVE- 2026- 28119	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Nirvana nirvana allows PHP Local File Inclusion.This issue affects Nirvana: from n/a through <= 2.6.	8.1	More Details
CVE- 2026- 28118	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Welldone welldone allows PHP Local File Inclusion.This issue affects Welldone: from n/a through <= 2.4.	8.1	More Details
CVE- 2026- 28117	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes smart SEO smartSEO allows PHP Local File Inclusion.This issue affects smart SEO: from n/a through <= 2.9.	8.1	More Details
CVE- 2026- 28107	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Muzicon muzicon allows PHP Local File Inclusion.This issue affects Muzicon: from n/a through <= 1.9.0.	8.1	More Details
CVE- 2026- 28098	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Save Life save-life allows PHP Local File Inclusion.This issue affects Save Life: from n/a through <= 1.2.13.	8.1	More Details
CVE- 2026- 28097	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Artrium artrium allows PHP Local File Inclusion.This issue affects Artrium: from n/a through <= 1.0.14.	8.1	More Details
CVE- 2026- 28096	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX WealthCo wealthco allows PHP Local File Inclusion.This issue affects WealthCo: from n/a through <= 2.18.	8.1	More Details
CVE- 2026- 28095	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Marcell marcell allows PHP Local File Inclusion.This issue affects Marcell: from n/a through <= 1.2.14.	8.1	More Details
CVE- 2026- 28093	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Ozisti ozisti allows PHP Local File Inclusion.This issue affects Ozisti: from n/a through <= 1.1.10.	8.1	More Details
CVE- 2026- 28123	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Veil veil allows PHP Local File Inclusion.This issue affects Veil: from n/a through <= 1.9.	8.1	More Details
CVE- 2026- 28092	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Sounder sounder allows PHP Local File Inclusion.This issue affects Sounder: from n/a through <= 1.3.11.	8.1	More Details
CVE- 2026- 28091	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Coleo coleo allows PHP Local File Inclusion.This issue affects Coleo: from n/a through <= 1.1.7.	8.1	More Details
CVE- 2025-	A Stack-based Buffer Overflow vulnerability [CWE-121] vulnerability in Fortinet FortiManager 7.4.0 through 7.4.2, FortiManager 7.2.0 through 7.2.10, FortiManager 6.4 all versions may allow a remote unauthenticated attacker to execute unauthorized commands via crafted requests, if the service is	8.1	More Details

54820	enabled. The success of the attack depends on the ability to bypass the stack protection mechanisms.		
CVE-2026-28090	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Gamezone gamezone allows PHP Local File Inclusion.This issue affects Gamezone: from n/a through <= 1.1.11.	8.1	More Details
CVE-2026-28029	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX EmojiNation emojination allows PHP Local File Inclusion.This issue affects EmojiNation: from n/a through <= 1.0.12.	8.1	More Details
CVE-2026-28088	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Aqualots aqualots allows PHP Local File Inclusion.This issue affects Aqualots: from n/a through <= 1.1.6.	8.1	More Details
CVE-2026-28087	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Filmax filmax allows PHP Local File Inclusion.This issue affects Filmax: from n/a through <= 1.1.11.	8.1	More Details
CVE-2026-28086	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Run Gran run-gran allows PHP Local File Inclusion.This issue affects Run Gran: from n/a through <= 2.0.	8.1	More Details
CVE-2026-22435	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes ElectroServ electroserv allows PHP Local File Inclusion.This issue affects ElectroServ: from n/a through <= 1.3.2.	8.1	More Details
CVE-2026-28084	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Bazinga bazinga allows PHP Local File Inclusion.This issue affects Bazinga: from n/a through <= 1.1.9.	8.1	More Details
CVE-2026-24017	An Improper Control of Interaction Frequency vulnerability [CWE-799] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4.0 through 7.4.10, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow a remote unauthenticated attacker to bypass the authentication rate-limit via crafted requests. The success of the attack depends on the attacker's resources and the password target complexity.	8.1	More Details
CVE-2026-28124	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Notarius notarius allows PHP Local File Inclusion.This issue affects Notarius: from n/a through <= 1.9.	8.1	More Details
CVE-2026-28081	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Windsor windsor allows PHP Local File Inclusion.This issue affects Windsor: from n/a through <= 2.5.0.	8.1	More Details
CVE-2026-3009	A security flaw in the IdentityBrokerService.performLogin endpoint of Keycloak allows authentication to proceed using an Identity Provider (IdP) even after it has been disabled by an administrator. An attacker who knows the IdP alias can reuse a previously generated login request to bypass the administrative restriction. This undermines access control enforcement and may allow unauthorized authentication through a disabled external provider.	8.1	More Details
CVE-2025-59541	Chamilo is a learning management system. Prior to version 1.11.34, a Cross-Site Request Forgery (CSRF) vulnerability allows an attacker to delete projects inside a course without the victim’s consent. The issue arises because sensitive actions such as project deletion do not implement anti-CSRF protections (tokens) and GET based requests. As a result, an authenticated user (Trainer) can be tricked into executing this unwanted action by simply visiting a malicious page. This issue has been patched in version 1.11.34.	8.1	More Details
CVE-2026-29093	WWBN AVideo is an open source video platform. Prior to version 24.0, the official docker-compose.yml publishes the memcached service on host port 11211 (0.0.0.0:11211) with no authentication, while the Dockerfile configures PHP to store all user sessions in that memcached instance. An attacker who can reach port 11211 can read, modify, or flush session data — enabling session hijacking, admin impersonation, and mass session destruction without any application-level authentication. This issue has been patched in version 24.0.	8.1	More Details
CVE-	Internet Routing Registry daemon version 4 is an IRR database server, processing IRR objects in the RPSL format. From version 4.4.0 to before version 4.4.5 and from version 4.5.0 to before version 4.5.1, an attacker can manipulate the HTTP Host header on a password reset or account creation request. The confirmation link in the resulting email can then point to an attacker-controlled domain. Opening the link in the email is sufficient to pass the token to the attacker, who can then use it on the real IRRD		More

2026-28681	instance to take over the account. A compromised account can then be used to modify RPSL objects maintained by the account's mntners and perform other account actions. If the user had two-factor authentication configured, which is required for users with override access, an attacker is not able to log in, even after successfully resetting the password. This issue has been patched in versions 4.4.5 and 4.5.1.	8.1	Details
CVE-2026-28473	OpenClaw versions prior to 2026.2.2 contain an authorization bypass vulnerability where clients with operator.write scope can approve or deny exec approval requests by sending the /approve chat command. The /approve command path invokes exec.approval.resolve through an internal privileged gateway client, bypassing the operator.approvals permission check that protects direct RPC calls.	8.1	More Details
CVE-2026-28472	OpenClaw versions prior to 2026.2.2 contain a vulnerability in the gateway WebSocket connect handshake in which it allows skipping device identity checks when auth.token is present but not validated. Attackers can connect to the gateway without providing device identity or pairing by exploiting the presence check instead of validation, potentially gaining operator access in vulnerable deployments.	8.1	More Details
CVE-2026-28458	OpenClaw version 2026.1.20 prior to 2026.2.1 contains a vulnerability in the Browser Relay (extension must be installed and enabled) /cdp WebSocket endpoint in which it does not require authentication tokens, allowing websites to connect via loopback and access sensitive data. Attackers can exploit this by connecting to ws://127.0.0.1:18792/cdp to steal session cookies and execute JavaScript in other browser tabs.	8.1	More Details
CVE-2026-28447	OpenClaw versions 2026.1.29-beta.1 prior to 2026.2.1 contain a path traversal vulnerability in plugin installation that allows malicious plugin package names to escape the extensions directory. Attackers can craft scoped package names containing path traversal sequences like .. to write files outside the intended installation directory when victims run the plugins install command.	8.1	More Details
CVE-2026-28410	The Graph is an indexing protocol for querying networks like Ethereum, IPFS, Polygon, and other blockchains. Prior to version 3.0.0, a flaw in the token vesting contracts allows users to access tokens that should still be locked according to their vesting schedule. This issue has been patched in version 3.0.0.	8.1	More Details
CVE-2025-70614	OpenCode Systems OC Messaging / USSD Gateway OC Release 6.32.2 contains a broken access control vulnerability in the web-based control panel allowing authenticated low-privileged attackers to gain to access to arbitrary SMS messages via a crafted company or tenant identifier parameter.	8.1	More Details
CVE-2026-3459	The Drag and Drop Multiple File Upload - Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'dnd_upload_cf7_upload' function in versions up to, and including, 1.3.7.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This can be exploited if the form includes a multiple file upload field with ‘*’ as the accepted file type.	8.1	More Details
CVE-2026-26148	External initialization of trusted variables or data stores in Azure Entra ID allows an unauthorized attacker to elevate privileges locally.	8.1	More Details
CVE-2026-28125	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Midi midi allows PHP Local File Inclusion.This issue affects Midi: from n/a through <= 1.14.	8.1	More Details
CVE-2026-26417	A broken access control vulnerability in the password reset functionality of Tata Consultancy Services Cognix Recon Client v3.0 allows authenticated users to reset passwords of arbitrary user accounts via crafted requests.	8.1	More Details
CVE-2026-29091	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Prior to version 3.0.0, a remote code execution (RCE) flaw was discovered in the locutus project, specifically within the call_user_func_array function implementation. The vulnerability allows an attacker to inject arbitrary JavaScript code into the application's runtime environment. This issue stems from an insecure implementation of the call_user_func_array function (and its wrapper call_user_func), which fails to properly validate all components of a callback array before passing them to eval(). This issue has been patched in version 3.0.0.	8.1	More Details
CVE-2026-29067	ZITADEL is an open source identity management platform. From version 4.0.0-rc.1 to 4.7.0, a potential vulnerability exists in ZITADEL's password reset mechanism in login V2. ZITADEL utilizes the Forwarded or X-Forwarded-Host header from incoming requests to construct the URL for the password reset confirmation link. This link, containing a secret code, is then emailed to the user. This issue has been patched in version 4.7.1.	8.1	More Details

CVE-2026-26105	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-2026-20002	A vulnerability in the web-based management interface of Cisco Secure FMC Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to inadequate validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted requests to an affected device. A successful exploit could allow the attacker to obtain full access to the database and read certain files on the underlying operating system. To exploit this vulnerability, the attacker would need valid user credentials.	8.1	More Details
CVE-2026-28678	DSA Study Hub is an interactive educational web application. Prior to commit d527fba, the user authentication system in server/routes/auth.js was found to be vulnerable to Insufficiently Protected Credentials. Authentication tokens (JWTs) were stored in HTTP cookies without cryptographic protection of the payload. This issue has been patched via commit d527fba.	8.1	More Details
CVE-2026-30851	Caddy is an extensible server platform that uses TLS by default. From version 2.10.0 to before version 2.11.2, forward_auth copy_headers does not strip client-supplied headers, allowing identity injection and privilege escalation. This issue has been patched in version 2.11.2.	8.1	More Details
CVE-2026-1321	The Membership Plugin – Restrict Content plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.2.20. This is due to the `rcp_setup_registration_init()` function accepting any membership level ID via the `rcp_level` POST parameter without validating that the level is active or that payment is required. Combined with the `add_user_role()` method which assigns the WordPress role configured on the membership level without status checks, this makes it possible for unauthenticated attackers to register with any membership level, including inactive levels that grant privileged WordPress roles such as Administrator, or paid levels that charge a sign-up fee. The vulnerability was partially patched in version 3.2.18.	8.1	More Details
CVE-2026-28129	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Little Birdies little-birdies allows PHP Local File Inclusion.This issue affects Little Birdies: from n/a through <= 1.3.16.	8.1	More Details
CVE-2026-28128	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Verse verse allows PHP Local File Inclusion.This issue affects Verse: from n/a through <= 1.7.0.	8.1	More Details
CVE-2026-28693	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, an integer overflow in DIB coder can result in out of bounds read or write. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	8.1	More Details
CVE-2026-28085	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Mahogany mahogany allows PHP Local File Inclusion.This issue affects Mahogany: from n/a through <= 2.9.	8.1	More Details
CVE-2026-28079	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Conquerors conquerors allows PHP Local File Inclusion.This issue affects Conquerors: from n/a through <= 1.2.13.	8.1	More Details
CVE-2026-22420	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Horizon horizon allows PHP Local File Inclusion.This issue affects Horizon: from n/a through <= 1.1.	8.1	More Details
CVE-2026-22408	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Justicia justicia allows PHP Local File Inclusion.This issue affects Justicia: from n/a through <= 1.2.	8.1	More Details
CVE-2026-28077	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Vapester vapester allows PHP Local File Inclusion.This issue affects Vapester: from n/a through <= 1.1.10.	8.1	More Details
CVE-2026-22412	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Eona eona allows PHP Local File Inclusion.This issue affects Eona: from n/a through <= 1.3.	8.1	More Details
CVE-2026-22413	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Malgré malgre allows PHP Local File Inclusion.This issue affects Malgré: from n/a through <= 1.0.3.	8.1	More Details

CVE-2026-22414	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Marra marra allows PHP Local File Inclusion.This issue affects Marra: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22415	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes The Mounty the-mounty allows PHP Local File Inclusion.This issue affects The Mounty: from n/a through <= 1.1.	8.1	More Details
CVE-2026-22416	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes FixTeam fixteam allows PHP Local File Inclusion.This issue affects FixTeam: from n/a through <= 1.4.	8.1	More Details
CVE-2026-22417	Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Wedding grandwedding allows Object Injection.This issue affects Grand Wedding: from n/a through <= 3.1.0.	8.1	More Details
CVE-2026-22418	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Great Lotus great-lotus allows PHP Local File Inclusion.This issue affects Great Lotus: from n/a through <= 1.3.1.	8.1	More Details
CVE-2026-22419	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Honor honor allows PHP Local File Inclusion.This issue affects Honor: from n/a through <= 2.3.	8.1	More Details
CVE-2026-22421	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Quantum quantum allows PHP Local File Inclusion.This issue affects Quantum: from n/a through <= 1.0.	8.1	More Details
CVE-2026-22403	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Innovio innovio allows PHP Local File Inclusion.This issue affects Innovio: from n/a through <= 1.7.	8.1	More Details
CVE-2026-22423	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes SetSail setsail allows PHP Local File Inclusion.This issue affects SetSail: from n/a through <= 1.8.	8.1	More Details
CVE-2026-22424	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Shaha shaha allows PHP Local File Inclusion.This issue affects Shaha: from n/a through <= 1.1.2.	8.1	More Details
CVE-2026-22425	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Sweet Jane sweetjane allows PHP Local File Inclusion.This issue affects Sweet Jane: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22427	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes GoTravel gotravel allows PHP Local File Inclusion.This issue affects GoTravel: from n/a through <= 2.1.	8.1	More Details
CVE-2026-22428	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Tooth Fairy tooth-fairy allows PHP Local File Inclusion.This issue affects Tooth Fairy: from n/a through <= 1.16.	8.1	More Details
CVE-2026-22429	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Verdure verdure allows PHP Local File Inclusion.This issue affects Verdure: from n/a through <= 1.6.	8.1	More Details
CVE-2026-22431	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Wabi-Sabi wabi-sabi allows PHP Local File Inclusion.This issue affects Wabi-Sabi: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22432	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Woopy woopy allows PHP Local File Inclusion.This issue affects Woopy: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22433	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes CloudMe cloudme allows PHP Local File Inclusion.This issue affects CloudMe: from n/a through <= 1.2.2.	8.1	More Details
CVE-2026-22434	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Crown Art crown-art allows PHP Local File Inclusion.This issue affects Crown Art: from n/a through <= 1.2.11.	8.1	More Details

CVE-2026-28057	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Mandala mandala allows PHP Local File Inclusion.This issue affects Mandala: from n/a through <= 2.8.	8.1	More Details
CVE-2026-22410	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Dolcino dolcino allows PHP Local File Inclusion.This issue affects Dolcino: from n/a through <= 1.6.	8.1	More Details
CVE-2026-22399	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Holmes holmes allows PHP Local File Inclusion.This issue affects Holmes: from n/a through <= 1.7.	8.1	More Details
CVE-2026-22397	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Fleur fleur allows PHP Local File Inclusion.This issue affects Fleur: from n/a through <= 2.0.	8.1	More Details
CVE-2026-28069	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Le Truffe letruffe allows PHP Local File Inclusion.This issue affects Le Truffe: from n/a through <= 1.1.7.	8.1	More Details
CVE-2026-28068	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Rhythmo rhythmo allows PHP Local File Inclusion.This issue affects Rhythmo: from n/a through <= 1.3.4.	8.1	More Details
CVE-2026-28067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Bassein bassein allows PHP Local File Inclusion.This issue affects Bassein: from n/a through <= 1.0.15.	8.1	More Details
CVE-2026-28066	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Legrand legrand allows PHP Local File Inclusion.This issue affects Legrand: from n/a through <= 2.17.	8.1	More Details
CVE-2026-28065	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Eject eject allows PHP Local File Inclusion.This issue affects Eject: from n/a through <= 2.17.	8.1	More Details
CVE-2026-28064	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Edge Decor edge-decor allows PHP Local File Inclusion.This issue affects Edge Decor: from n/a through <= 2.2.	8.1	More Details
CVE-2026-28063	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Asia Garden asia-garden allows PHP Local File Inclusion.This issue affects Asia Garden: from n/a through <= 1.3.1.	8.1	More Details
CVE-2026-28062	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Happy Baby happy-baby allows PHP Local File Inclusion.This issue affects Happy Baby: from n/a through <= 1.2.12.	8.1	More Details
CVE-2026-28061	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Tiger Claw tiger-claw allows PHP Local File Inclusion.This issue affects Tiger Claw: from n/a through <= 1.1.14.	8.1	More Details
CVE-2025-53335	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Berger berger allows PHP Local File Inclusion.This issue affects Berger: from n/a through <= 1.1.1.	8.1	More Details
CVE-2025-69090	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ovatheme Remons remons allows PHP Local File Inclusion.This issue affects Remons: from n/a through <= 1.3.4.	8.1	More Details
CVE-2025-69339	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in don-themes Molla molla allows PHP Local File Inclusion.This issue affects Molla: from n/a through <= 1.5.16.	8.1	More Details
CVE-2026-28060	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX S.King stephanie-king allows PHP Local File Inclusion.This issue affects S.King: from n/a through <= 1.5.3.	8.1	More Details
CVE-2026-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Dermatology Clinic dermatology-clinic allows PHP Local File	8.1	More

28059	Inclusion.This issue affects Dermatology Clinic: from n/a through <= 1.4.3.		Details
CVE-2026-28058	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Dixon dixon allows PHP Local File Inclusion.This issue affects Dixon: from n/a through <= 1.4.2.1.	8.1	More Details
CVE-2026-22385	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in don-themes Wolmart wolmart allows PHP Local File Inclusion.This issue affects Wolmart: from n/a through <= 1.9.6.	8.1	More Details
CVE-2026-22387	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Aviana aviana allows PHP Local File Inclusion.This issue affects Aviana: from n/a through <= 2.1.	8.1	More Details
CVE-2026-22389	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Cocco cocco allows PHP Local File Inclusion.This issue affects Cocco: from n/a through <= 1.5.1.	8.1	More Details
CVE-2026-22392	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Cortex cortex allows PHP Local File Inclusion.This issue affects Cortex: from n/a through <= 1.5.	8.1	More Details
CVE-2026-22394	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Evently evently allows PHP Local File Inclusion.This issue affects Evently: from n/a through <= 1.7.	8.1	More Details
CVE-2026-22395	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Fiorello fiorello allows PHP Local File Inclusion.This issue affects Fiorello: from n/a through <= 1.0.	8.1	More Details
CVE-2026-28028	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX MoneyFlow moneyflow allows PHP Local File Inclusion.This issue affects MoneyFlow: from n/a through <= 1.0.	8.1	More Details
CVE-2025-15558	Docker CLI for Windows searches for plugin binaries in C:\ProgramData\Docker\cli-plugins, a directory that does not exist by default. A low-privileged attacker can create this directory and place malicious CLI plugin binaries (docker-compose.exe, docker-buildx.exe, etc.) that are executed when a victim user opens Docker Desktop or invokes Docker CLI plugin features, and allow privilege-escalation if the docker CLI is executed as a privileged user. This issue affects Docker CLI: through 29.1.5 and Windows binaries acting as a CLI-plugin manager using the github.com/docker/cli/cli-plugins/manager https://pkg.go.dev/github.com/docker/cli@v29.1.5+incompatible/cli-plugins/manager package, such as Docker Compose. This issue does not impact non-Windows binaries, and projects not using the plugin-manager code.	8.0	More Details
CVE-2026-28405	MarkUs is a web application for the submission and grading of student assignments. Prior to version 2.9.1, the courses/<:course_id>/assignments/<:assignment_id>/submissions/html_content route reads the contents of a student-submitted file and renders them without sanitization. This issue has been patched in version 2.9.1.	8.0	More Details
CVE-2026-25173	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-70616	A stack buffer overflow vulnerability exists in the Wincor Nixdorf wnBios64.sys kernel driver (version 1.2.0.0) in the IOCTL handler for code 0x80102058. The vulnerability is caused by missing bounds checking on the user-controlled Options parameter before copying data into a 40-byte stack buffer (Src[40]) using memmove. An attacker with local access can exploit this vulnerability by sending a crafted IOCTL request with Options > 40, causing a stack buffer overflow that may lead to kernel code execution, local privilege escalation, or denial of service (system crash). Additionally, the same IOCTL handler can leak kernel addresses and other sensitive stack data when reading beyond the buffer boundaries.	7.8	More Details
CVE-2026-27750	Avira Internet Security contains a time-of-check time-of-use (TOCTOU) vulnerability in the Optimizer component. A privileged service running as SYSTEM identifies directories for cleanup during a scan phase and subsequently deletes them during a separate cleanup phase without revalidating the target path. A local attacker can replace a previously scanned directory with a junction or reparse point before deletion occurs, causing the privileged process to delete an unintended system location. This may result in deletion of protected files or directories and can lead to local privilege escalation, denial of service, or system integrity compromise depending on the affected target.	7.8	More Details

CVE-2026-27749	Avira Internet Security contains a deserialization of untrusted data vulnerability in the System Speedup component. The Avira.SystemSpeedup.RealTimeOptimizer.exe process, which runs with SYSTEM privileges, deserializes data from a file located in C:\\ProgramData using .NET BinaryFormatter without implementing input validation or deserialization safeguards. Because the file can be created or modified by a local user in default configurations, an attacker can supply a crafted serialized payload that is deserialized by the privileged process, resulting in arbitrary code execution as SYSTEM.	7.8	More Details
CVE-2026-27748	Avira Internet Security contains an improper link resolution vulnerability in the Software Updater component. During the update process, a privileged service running as SYSTEM deletes a file under C:\\ProgramData without validating whether the path resolves through a symbolic link or reparse point. A local attacker can create a malicious link to redirect the delete operation to an arbitrary file, resulting in deletion of attacker-chosen files with SYSTEM privileges. This may lead to local privilege escalation, denial of service, or system integrity compromise depending on the targeted file and operating system configuration.	7.8	More Details
CVE-2026-27272	Illustrator versions 29.8.4, 30.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-70341	Insecure permissions in App-Auto-Patch v3.4.2 create a race condition which allows attackers to write arbitrary files.	7.8	More Details
CVE-2026-30983	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a stack buffer overflow in icFixXml() (strcpy) causing stack memory corruption or crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-24290	Improper access control in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24289	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24287	External control of file name or path in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24018	A UNIX symbolic link (Symlink) following vulnerability in Fortinet FortiClientLinux 7.4.0 through 7.4.4, FortiClientLinux 7.2.2 through 7.2.12 may allow a local and unprivileged user to escalate their privileges to root.	7.8	More Details
CVE-2026-23673	Out-of-bounds read in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-23672	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2026-23665	Heap-based buffer overflow in Azure Linux Virtual Machines allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-30978	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-use-after-free in CIccCmm::AddXform() causing invalid vptr dereference and crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-30979	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-based buffer overflow in CIccCalculatorFunc::InitSelectOp() triggered with local user interaction causing memory corruption/crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-30985	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-based buffer overflow write in CIccMatrixMath::SetRange() causing memory corruption or crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-	Substance3D - Stager versions 3.1.7 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue	7.8	More Details

27276	requires user interaction in that a victim must open a malicious file.		
CVE-2026-30987	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a stack buffer overflow in CIccTagNum<>::GetValues() causing stack memory corruption or crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-31792	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a null pointer dereference in CIccTagXmlStruct::ParseTag() causing a segmentation fault or denial of service. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-31795	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a stack buffer overflow write in CIccXform3DLut::Apply() corrupting stack memory or crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-31796	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-based buffer overflow in icCurvesFromXml() causing heap memory corruption or crash. This vulnerability is fixed in 2.3.1.5.	7.8	More Details
CVE-2026-3483	An exposed dangerous method in Ivanti DSM before version 2026.1.1 allows a local authenticated attacker to escalate their privileges.	7.8	More Details
CVE-2026-23660	Improper access control in Azure Portal Windows Admin Center allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27269	Premiere Pro versions 25.5 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27273	Substance3D - Stager versions 3.1.7 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27274	Substance3D - Stager versions 3.1.7 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-24291	Incorrect permission assignment for critical resource in Windows Accessibility Infrastructure (ATBroker.exe) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24292	Use after free in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24293	Null pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-24294	Improper authentication in Windows SMB Server allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26112	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-27278	Acrobat Reader versions 24.001.30307, 24.001.30308, 25.001.21265 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-26128	Improper authentication in Windows SMB Server allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26131	Incorrect default permissions in .NET allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2026-26108	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-26107	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-26132	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26134	Integer overflow or wraparound in Microsoft Office allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26141	Improper authentication in Azure Arc allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26738	Buffer Overflow vulnerability in Uderzo Software SpaceSniffer v.2.0.5.18 allows a remote attacker to execute arbitrary code via a crafted .sns snapshot file.	7.8	More Details
CVE-2026-25190	Untrusted search path in Windows GDI allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-25189	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-25187	Improper link resolution before file access ('link following') in Winlogon allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27220	Acrobat Reader versions 24.001.30307, 24.001.30308, 25.001.21265 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-25176	Improper access control in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-25175	Out-of-bounds read in Windows NTFS allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-25174	Out-of-bounds read in Windows Extensible File Allocation allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-25166	Deserialization of untrusted data in Windows System Image Manager allows an authorized attacker to execute code locally.	7.8	More Details
CVE-2026-25165	Null pointer dereference in Windows Performance Counters allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27275	Substance3D - Stager versions 3.1.7 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-26117	Authentication bypass using an alternate path or channel in Azure Windows Virtual Machine Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27280	DNG SDK versions 1.7.1 2471 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE-2026-27271	Illustrator versions 29.8.4, 30.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27277	Substance3D - Stager versions 3.1.7 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-25866	MobaXterm versions prior to 26.1 contain an uncontrolled search path element vulnerability. The application calls WinExec to execute Notepad++ without a fully qualified executable path when opening remote files. An attacker can exploit the search path behavior by placing a malicious executable earlier in the search order, resulting in arbitrary code execution in the context of the affected user.	7.8	More Details
CVE-2025-41761	A low-privileged local attacker who gains access to the UBR service account (e.g., via SSH) can escalate privileges to obtain full system access. This is due to the service account being permitted to execute certain binaries (e.g., tcpdump and ip) with sudo.	7.8	More Details
CVE-2026-27267	Illustrator versions 29.8.4, 30.1 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-3094	Delta Electronics CNCSoft-G2 lacks proper validation of the user-supplied file. If a user opens a malicious file, an attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2026-29127	The IDC SFX2100 Satellite Receiver sets overly permissive file system permissions on the monitor user's home directory. The directory is configured with permissions 0777, granting read, write, and execute access to all local users on the system, which may cause local privilege escalation depending on conditions of the system due to the presence of highly privileged processes and binaries residing within the affected directory.	7.8	More Details
CVE-2026-21362	Illustrator versions 29.8.4, 30.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27279	Substance3D - Stager versions 3.1.7 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27689	Due to an uncontrolled resource consumption (Denial of Service) vulnerability, an authenticated attacker with regular user privileges and network access can repeatedly invoke a remote-enabled function module with an excessively large loop-control parameter. This triggers prolonged loop execution that consumes excessive system resources, potentially rendering the system unavailable. Successful exploitation results in a denial-of-service condition that impacts availability, while confidentiality and integrity remain unaffected.	7.7	More Details
CVE-2026-20105	A vulnerability in the Remote Access SSL VPN functionality of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker with a valid VPN connection to exhaust device memory resulting in a denial of service (DoS) condition.This does not affect the management or MUS interfaces. This vulnerability is due to trusting user input without validation. An attacker could exploit this vulnerability by sending crafted packets to the Remote Access SSL VPN server. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	7.7	More Details
CVE-2026-20100	A vulnerability in the LUA interperter of the Remote Access SSL VPN feature of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker with a valid VPN connection to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This does not affect the management or MUS interfaces. This vulnerability is due to trusting user input without validation in the LUA interprerter. An attacker could exploit this vulnerability by sending crafted HTTP packets to the Remote Access SSL VPN server. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	7.7	More Details
CVE-	A vulnerability in the processing of Galois/Counter Mode (GCM)-encrypted Internet Key Exchange version 2 (IKEv2) IPsec traffic of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to the		More

2026-20049	allocation of an insufficiently sized block of memory. An attacker could exploit this vulnerability by sending crafted GCM-encrypted IPsec traffic to an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. To exploit this vulnerability, the attacker must have valid credentials to establish a VPN connection with the affected device.	7.7	Details
CVE-2026-30929	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, MagnifyImage uses a fixed-size stack buffer. When using a specific image it is possible to overflow this buffer and corrupt the stack. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	7.7	More Details
CVE-2026-26017	CoreDNS is a DNS server that chains plugins. Prior to version 1.14.2, a logical vulnerability in CoreDNS allows DNS access controls to be bypassed due to the default execution order of plugins. Security plugins such as acl are evaluated before the rewrite plugin, resulting in a Time-of-Check Time-of-Use (TOCTOU) flaw. This issue has been patched in version 1.14.2.	7.7	More Details
CVE-2026-20014	A vulnerability in the IKEv2 feature of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an authenticated, remote attacker with valid VPN user credentials to cause a DoS condition on an affected device that may also impact the availability of services to devices elsewhere in the network. This vulnerability is due to the improper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted, authenticated IKEv2 packets to an affected device. A successful exploit could allow the attacker to exhaust memory, causing the device to reload.	7.7	More Details
CVE-2026-29192	ZITADEL is an open source identity management platform. From version 4.0.0 to 4.11.1, a vulnerability in Zitadel's login V2 interface was discovered that allowed a possible account takeover via Default URI Redirect. This issue has been patched in version 4.12.0.	7.7	More Details
CVE-2026-29186	Backstage is an open framework for building developer portals. Prior to version 1.14.3, this is a configuration bypass vulnerability that enables arbitrary code execution. The @backstage/plugin-techdocs-node package uses an allowlist to filter dangerous MkDocs configuration keys during the documentation build process. A gap in this allowlist allows attackers to craft an mkdocs.yml that causes arbitrary Python code execution, completely bypassing TechDocs' security controls. This issue has been patched in version 1.14.3.	7.7	More Details
CVE-2026-31801	zot is ancontainer image/artifact registry based on the Open Container Initiative Distribution Specification. From 1.3.0 to 2.1.14, zot’s dist-spec authorization middleware infers the required action for PUT /v2/{name}/manifests/{reference} as create by default, and only switches to update when the tag already exists and reference != "latest". As a result, when latest already exists, a user who is allowed to create (but not allowed to update) can still pass the authorization check for an overwrite attempt of latest. This vulnerability is fixed in 2.1.15.	7.7	More Details
CVE-2026-28468	OpenClaw versions 2026.1.29-beta.1 prior to 2026.2.14 contain a vulnerability in the sandbox browser bridge server in which it accepts requests without requiring gateway authentication, allowing local attackers to access browser control endpoints. A local attacker can enumerate tabs, retrieve WebSocket URLs, execute JavaScript, and exfiltrate cookies and session data from authenticated browser contexts.	7.7	More Details
CVE-2026-30953	LinkAce is a self-hosted archive to collect website links. When a user creates a link via POST /links, the server fetches HTML metadata from the provided URL (LinkRepository::create() calls HtmlMeta::getFromUrl()). The LinkStoreRequest validation rules do not include NoPrivateIpRule, allowing server-side requests to internal network addresses, Docker service hostnames, and cloud metadata endpoints. The project already has a NoPrivateIpRule class (app/Rules/NoPrivateIpRule.php) but it is only applied in FetchController.php (line 99), not in the primary link creation path.	7.7	More Details
CVE-2026-28393	OpenClaw versions 2.0.0-beta3 prior to 2026.2.14 contain a path traversal vulnerability in hook transform module loading that allows arbitrary JavaScript execution. The hooks.mappings[].transform.module parameter accepts absolute paths and traversal sequences, enabling attackers with configuration write access to load and execute malicious modules with gateway process privileges.	7.7	More Details
CVE-2026-29053	Ghost is a Node.js content management system. From version 0.7.2 to 6.19.0, specifically crafted malicious themes can execute arbitrary code on the server running Ghost. This issue has been patched in version 6.19.1.	7.6	More Details
CVE-2026-30918	facileManager is a modular suite of web apps built with the sysadmin in mind. Prior to 6.0.4 , a reflected XSS occurs when an application receives data from an untrusted source and uses it in its HTTP responses in a way that could lead to vulnerabilities. It is possible to inject malicious JavaScript code into a URL by adding a script in a parameter. This vulnerability was found in the fmDNS module. The parameter that is vulnerable to an XSS attack is log_search_query. This vulnerability is fixed in	7.6	More Details

	6.0.4.		
CVE-2026-30919	facileManager is a modular suite of web apps built with the sysadmin in mind. Prior to 6.0.4 , stored XSS (also known as persistent or second-order XSS) occurs when an application receives data from an untrusted source and includes that data in its subsequent HTTP responses in an unsafe manner. This vulnerability was found in the fmDNS module. This vulnerability is fixed in 6.0.4.	7.6	More Details
CVE-2025-70244	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the webPage parameter to goform/formWlanSetup.	7.5	More Details
CVE-2026-29087	@hono/node-server allows running the Hono application on Node.js. Prior to version 1.19.10, when using @hono/node-server's static file serving together with route-based middleware protections (e.g. protecting /admin/*), inconsistent URL decoding can allow protected static resources to be accessed without authorization. In particular, paths containing encoded slashes (%2F) may be evaluated differently by routing/middleware matching versus static file path resolution, enabling a bypass where middleware does not run but the static file is still served. This issue has been patched in version 1.19.10.	7.5	More Details
CVE-2026-26999	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.38 and 3.6.9, there is a potential vulnerability in Traefik managing TLS handshake on TCP routers. When Traefik processes a TLS connection on a TCP router, the read deadline used to bound protocol sniffing is cleared before the TLS handshake is completed. When a TLS handshake read error occurs, the code attempts a second handshake with different connection parameters, silently ignoring the initial error. A remote unauthenticated client can exploit this by sending an incomplete TLS record and stopping further data transmission, causing the TLS handshake to stall indefinitely and holding connections open. By opening many such stalled connections in parallel, an attacker can exhaust file descriptors and goroutines, degrading availability of all services on the affected entrypoint. This issue has been patched in versions 2.11.38 and 3.6.9.	7.5	More Details
CVE-2026-29062	jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. From version 3.0.0 to before version 3.1.0, the UTF8DataInputJsonParser, which is used when parsing from a java.io.DataInput source, bypasses the maxNestingDepth constraint (default: 500) defined in StreamReadConstraints. A similar issue was found in ReaderBasedJsonParser. This allows a user to supply a JSON document with excessive nesting, which can cause a StackOverflowError when the structure is processed, leading to a Denial of Service (DoS). This issue has been patched in version 3.1.0.	7.5	More Details
CVE-2026-29611	OpenClaw versions prior to 2026.2.14 contain a local file inclusion vulnerability in BlueBubbles extension (must be installed and enabled) media path handling that allows attackers to read arbitrary files from the local filesystem. The sendBlueBubblesMedia function fails to validate mediaPath parameters against an allowlist, enabling attackers to request sensitive files like /etc/passwd and exfiltrate them as media attachments.	7.5	More Details
CVE-2026-26144	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-28392	OpenClaw versions prior to 2026.2.14 contain a privilege escalation vulnerability in the Slack slash-command handler that incorrectly authorizes any direct message sender when dmPolicy is set to open (must be configured). Attackers can execute privileged slash commands via direct message to bypass allowlist and access-group restrictions.	7.5	More Details
CVE-2026-29054	Traefik is an HTTP reverse proxy and load balancer. From version 2.11.9 to 2.11.37 and from version 3.1.3 to 3.6.8, there is a potential vulnerability in Traefik managing the Connection header with X-Forwarded headers. When Traefik processes HTTP/1.1 requests, the protection put in place to prevent the removal of Traefik-managed X-Forwarded headers (such as X-Real-Ip, X-Forwarded-Host, X-Forwarded-Port, etc.) via the Connection header does not handle case sensitivity correctly. The Connection tokens are compared case-sensitively against the protected header names, but the actual header deletion operates case-insensitively. As a result, a remote unauthenticated client can use lowercase Connection tokens (e.g. Connection: x-real-ip) to bypass the protection and trigger the removal of Traefik-managed forwarded identity headers. This issue has been patched in versions 2.11.38 and 3.6.9.	7.5	More Details
CVE-2018-25178	Easyndexer 1.0 contains an arbitrary file download vulnerability that allows unauthenticated attackers to download sensitive files by manipulating the file parameter. Attackers can send POST requests to showtif.php with arbitrary file paths in the file parameter to retrieve system files like configuration and initialization files.	7.5	More Details

CVE-2026-29609	OpenClaw versions prior to 2026.2.14 contain a denial of service vulnerability in the fetchWithGuard function that allocates entire response payloads in memory before enforcing maxBytes limits. Remote attackers can trigger memory exhaustion by serving oversized responses without content-length headers to cause availability loss.	7.5	More Details
CVE-2026-28453	OpenClaw versions prior to 2026.2.14 fail to validate TAR archive entry paths during extraction, allowing path traversal sequences to write files outside the intended directory. Attackers can craft malicious archives with traversal sequences like ../../ to write files outside extraction boundaries, potentially enabling configuration tampering and code execution.	7.5	More Details
CVE-2026-29074	SVGO, short for SVG Optimizer, is a Node.js library and command-line application for optimizing SVG files. From version 2.1.0 to before version 2.8.1, from version 3.0.0 to before version 3.3.3, and before version 4.0.1, SVGO accepts XML with custom entities, without guards against entity expansion or recursion. This can result in a small XML file (811 bytes) stalling the application and even crashing the Node.js process with JavaScript heap out of memory. This issue has been patched in versions 2.8.1, 3.3.3, and 4.0.1.	7.5	More Details
CVE-2018-25181	Musicco 2.0.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary directories by manipulating the parent parameter. Attackers can supply directory traversal sequences in the parent parameter of the getAlbum endpoint to access sensitive system directories and download them as ZIP files.	7.5	More Details
CVE-2026-29068	PJSIP is a free and open source multimedia communication library written in C. Prior to version 2.17, there is a stack buffer overflow vulnerability when pjmedia-codec parses an RTP payload contain more frames than the caller-provided frames can hold. This issue has been patched in version 2.17.	7.5	More Details
CVE-2026-3589	The WooCommerce WordPress plugin from versions 5.4.0 to 10.5.2 does not properly handle batch requests, which could allow unauthenticated users to make a logged in admin call non store/WC REST endpoints, and create arbitrary admin users via a CSRF attack for example.	7.5	More Details
CVE-2026-26418	Missing authentication and authorization in the web API of Tata Consultancy Services Cognix Recon Client v3.0 allows remote attackers to access application functionality without restriction via the network.	7.5	More Details
CVE-2026-29039	changedetection.io is a free open source web page change detection tool. Prior to version 0.54.4, the changedetection.io application allows users to specify XPath expressions as content filters via the include_filters field. These XPath expressions are processed using the elementpath library which implements XPath 3.0/3.1 specification. XPath 3.0 includes the unparsed-text() function which can read arbitrary files from the filesystem. The application does not validate or sanitize XPath expressions to block dangerous functions, allowing an attacker to read any file accessible to the application process. This issue has been patched in version 0.54.4.	7.5	More Details
CVE-2026-28799	PJSIP is a free and open source multimedia communication library written in C. Prior to version 2.17, a heap use-after-free vulnerability exists in PJSIP's event subscription framework (evsub.c) that is triggered during presence unsubscription (SUBSCRIBE with Expires=0). This issue has been patched in version 2.17.	7.5	More Details
CVE-2026-26130	Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-26514	An Argument Injection vulnerability exists in bird-lg-go before commit 6187a4e. The traceroute module uses shlex.Split to parse user input without validation, allowing remote attackers to inject arbitrary flags (e.g., -w, -q) via the q parameter. This can be exploited to cause a Denial of Service (DoS) by exhausting system resources.	7.5	More Details
CVE-2026-26673	An issue in DJI Mavic Mini, Spark, Mavic Air, Mini, Mini SE 0.1.00.0500 and below allows a remote attacker to cause a denial of service via the DJI Enhanced-WiFi transmission subsystem	7.5	More Details
CVE-2026-30837	Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation and client-server communication. Prior to 1.4.26 , t.String({ format: 'url' }) is vulnerable to ReDoS. Repeating a partial url format (protocol and hostname) multiple times cause regex to slow down significantly. This vulnerability is fixed in 1.4.26.	7.5	More Details
CVE-2026-26127	Out-of-bounds read in .NET allows an unauthorized attacker to deny service over a network.	7.5	More Details
	Sequelize is a Node.js ORM tool. Prior to 6.37.8, there is SQL injection via unescaped cast type in		

CVE-2026-30951	JSON/JSONB where clause processing. The _traverseJSON() function splits JSON path keys on :: to extract a cast type, which is interpolated raw into CAST(... AS <type>) SQL. An attacker who controls JSON object keys can inject arbitrary SQL and exfiltrate data from any table. This vulnerability is fixed in 6.37.8.	7.5	More Details
CVE-2025-45691	An Arbitrary File Read vulnerability exists in the ImageTextPromptValue class in Exploding Gradients RAGAS v0.2.3 to v0.2.14. The vulnerability stems from improper validation and sanitization of URLs supplied in the retrieved_contexts parameter when handling multimodal inputs.	7.5	More Details
CVE-2026-30798	Insufficient Verification of Data Authenticity, Improper Handling of Exceptional Conditions vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (Heartbeat sync loop, strategy processing modules) allows Protocol Manipulation. This vulnerability is associated with program files src/hbbs_http/sync.Rs and program routines stop-service handler in heartbeat loop. This issue affects RustDesk Client: through 1.4.5.	7.5	More Details
CVE-2026-26121	Server-side request forgery (ssrf) in Azure IoT Explorer allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2026-25679	url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.	7.5	More Details
CVE-2026-2339	Missing Authentication for Critical Function vulnerability in TUBITAK BILGEM Software Technologies Research Institute Liderahenk allows Remote Code Inclusion, Privilege Abuse, Command Injection.This issue affects Liderahenk: before v3.4.0.	7.5	More Details
CVE-2025-70949	An observable timing discrepancy in @perfood/couch-auth v0.26.0 allows attackers to access sensitive information via a timing side-channel.	7.5	More Details
CVE-2026-27137	When verifying a certificate chain which contains a certificate containing multiple email address constraints which share common local portions but different domain portions, these constraints will not be properly applied, and only the last constraint will be considered.	7.5	More Details
CVE-2026-27443	SEPPmail Secure Email Gateway before version 15.0.1 does not properly sanitize the headers from S/MIME protected MIME entities, allowing an attacker to control trusted headers.	7.5	More Details
CVE-2026-28790	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.11.0, OliveTin allows an unauthenticated guest to terminate running actions through KillAction even when authRequireGuestsToLogin: true is enabled. Guests are correctly blocked from dashboard access, but can still call the KillAction RPC directly and successfully stop a running action. This is a broken access control issue that causes unauthorized denial of service against legitimate action executions. This issue has been patched in version 3000.11.0.	7.5	More Details
CVE-2026-28789	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.10.3, an unauthenticated denial-of-service vulnerability exists in OliveTin’s OAuth2 login flow. Concurrent requests to /oauth/login can trigger unsynchronized access to a shared registeredStates map, causing a Go runtime panic (fatal error: concurrent map writes) and process termination. This allows remote attackers to crash the service when OAuth2 is enabled. This issue has been patched in version 3000.10.3.	7.5	More Details
CVE-2025-70242	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the webPage parameter to goform/formSetWanPPTP.	7.5	More Details
CVE-2025-70246	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formVirtualServ.	7.5	More Details
CVE-2026-2747	SEPPmail Secure Email Gateway before version 15.0.1 decrypts inline PGP messages without isolating them from surrounding unencrypted content, allowing exposure of sensitive information to an unauthorized actor.	7.5	More Details
CVE-2026-	An Absolute Path Traversal vulnerability exists in Navtor NavBox. The application exposes an HTTP service that fails to properly sanitize user-supplied path input. Unauthenticated remote attackers can exploit this issue by submitting requests containing absolute filesystem paths. Successful exploitation allows the attacker to retrieve arbitrary files from the underlying filesystem, limited only by the	7.5	More Details

2753	privileges of the service process. This can lead to the exposure of sensitive configuration files and system information.		
CVE-2025-70227	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the nextPage parameter to goform/formLanguageChange.	7.5	More Details
CVE-2026-28462	OpenClaw versions prior to 2026.2.13 contain a vulnerability in the browser control API in which it accepts user-supplied output paths for trace and download files without consistently constraining writes to temporary directories. Attackers with API access can exploit path traversal in POST /trace/stop, POST /wait/download, and POST /download endpoints to write files outside intended temp roots.	7.5	More Details
CVE-2026-28469	OpenClaw versions prior to 2026.2.14 contain a webhook routing vulnerability in the Google Chat monitor component that allows cross-account policy context misrouting when multiple webhook targets share the same HTTP path. Attackers can exploit first-match request verification semantics to process inbound webhook events under incorrect account contexts, bypassing intended allowlists and session policies.	7.5	More Details
CVE-2018-25169	AMPPS 2.7 contains a denial of service vulnerability that allows remote attackers to crash the service by sending malformed data to the default HTTP port. Attackers can establish multiple socket connections and transmit invalid payloads to exhaust server resources and cause service unavailability.	7.5	More Details
CVE-2026-2754	Navtor NavBox exposes sensitive configuration and operational data due to missing authentication on HTTP API endpoints. An unauthenticated remote attacker with network access to the device can execute HTTP GET requests to TCP port 8080 to retrieve internal network parameters including ECDIS & OT Information, device identifiers, and service status logs.	7.5	More Details
CVE-2025-70247	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWizard1.	7.5	More Details
CVE-2026-27444	SEPPmail Secure Email Gateway before version 15.0.1 incorrectly interprets email addresses in the email headers, causing an interpretation conflict with other mail infrastructure that allows an attacker to fake the source of the email or decrypt it.	7.5	More Details
CVE-2023-7337	The JS Help Desk – AI-Powered Support & Ticketing System plugin for WordPress is vulnerable to SQL Injection via the 'js-support-ticket-token-tkstatus' cookie in version 2.8.2 due to an incomplete fix for CVE-2023-50839 where a second sink was left with insufficient escaping on the user supplied values and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-27442	The GINA web interface in SEPPmail Secure Email Gateway before version 15.0.1 does not properly check attachment filenames in GINA-encrypted emails, allowing an attacker to access files on the gateway.	7.5	More Details
CVE-2025-70363	Incorrect access control in the REST API of Ibexa & Ciril GROUP eZ Platform / Ciril Platform 2.x allows unauthenticated attackers to access sensitive data via enumerating object IDs.	7.5	More Details
CVE-2025-70249	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWizard2.	7.5	More Details
CVE-2026-28478	OpenClaw versions prior to 2026.2.13 contain a denial of service vulnerability in webhook handlers that buffer request bodies without strict byte or time limits. Remote unauthenticated attackers can send oversized JSON payloads or slow uploads to webhook endpoints causing memory pressure and availability degradation.	7.5	More Details
CVE-2026-28479	OpenClaw versions prior to 2026.2.15 use SHA-1 to hash sandbox identifier cache keys for Docker and browser sandbox configurations, which is deprecated and vulnerable to collision attacks. An attacker can exploit SHA-1 collisions to cause cache poisoning, allowing one sandbox configuration to be misinterpreted as another and enabling unsafe sandbox state reuse.	7.5	More Details
CVE-2026-	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain	7.5	More Details

20882	unauthorized access.		
CVE-2018-25193	Mongoose Web Server 6.9 contains a denial of service vulnerability that allows remote attackers to crash the service by establishing multiple socket connections. Attackers can repeatedly create connections to the default port and send malformed data to exhaust server resources and cause service unavailability.	7.5	More Details
CVE-2026-28342	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.10.2, the PasswordHash API endpoint allows unauthenticated users to trigger excessive memory allocation by sending concurrent password hashing requests. By issuing multiple parallel requests, an attacker can exhaust available container memory, leading to service degradation or complete denial of service (DoS). The issue occurs because the endpoint performs computationally and memory-intensive hashing operations without request throttling, authentication requirements, or resource limits. This issue has been patched in version 3000.10.2.	7.5	More Details
CVE-2026-24696	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-28454	OpenClaw versions prior to 2026.2.2 fail to validate webhook secrets in Telegram webhook mode (must be enabled), allowing unauthenticated HTTP POST requests to the webhook endpoint that trust attacker-controlled JSON payloads. Remote attackers can forge Telegram updates by spoofing message.from.id and chat.id fields to bypass sender allowlists and execute privileged bot commands.	7.5	More Details
CVE-2026-26018	CoreDNS is a DNS server that chains plugins. Prior to version 1.14.2, a denial of service vulnerability exists in CoreDNS's loop detection plugin that allows an attacker to crash the DNS server by sending specially crafted DNS queries. The vulnerability stems from the use of a predictable pseudo-random number generator (PRNG) for generating a secret query name, combined with a fatal error handler that terminates the entire process. This issue has been patched in version 1.14.2.	7.5	More Details
CVE-2018-25164	EverSync 0.5 contains an arbitrary file download vulnerability that allows unauthenticated attackers to access sensitive files by requesting them directly from the files directory. Attackers can send GET requests to the files directory to download database files like db.sq3 containing application data and credentials.	7.5	More Details
CVE-2026-2025	The Mail Mint WordPress plugin before 1.19.5 does not have authorization in one of its REST API endpoint, allowing unauthenticated users to call it and retrieve the email addresses of users on the blog	7.5	More Details
CVE-2026-26801	Server-Side Request Forgery (SSRF) vulnerability in pdfmake versions 0.3.0-beta.2 through 0.3.5 allows a remote attacker to obtain sensitive information via the src/URLResolver.js component. The fix was released in version 0.3.6 which introduces the setUrlAccessPolicy() method allowing server operators to define URL access rules. A warning is now logged when pdfmake is used server-side without a policy configured.	7.5	More Details
CVE-2025-70251	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the webPage parameter to goform/formWlanGuestSetup.	7.5	More Details
CVE-2026-26308	Envoy is a high-performance edge/middle/service proxy. Prior to 1.37.1, 1.36.5, 1.35.8, and 1.34.13, the Envoy RBAC (Role-Based Access Control) filter contains a logic vulnerability in how it validates HTTP headers when multiple values are present for the same header name. Instead of validating each header value individually, Envoy concatenates all values into a single comma-separated string. This behavior allows attackers to bypass RBAC policies—specifically "Deny" rules—by sending duplicate headers, effectively obscuring the malicious value from exact-match mechanisms. This vulnerability is fixed in 1.37.1, 1.36.5, 1.35.8, and 1.34.13.	7.5	More Details
CVE-2026-30933	FileBrowser Quantum is a free, self-hosted, web-based file manager. Prior to 1.3.1-beta and 1.2.2-stable, the remediation for CVE-2026-27611 is incomplete. Password protected shares still disclose tokenized downloadURL via /public/api/share/info. This vulnerability is fixed in 1.3.1-beta and 1.2.2-stable.	7.5	More Details
CVE-2026-27406	Insertion of Sensitive Information Into Sent Data vulnerability in Joe Dolson My Tickets my-tickets allows Retrieve Embedded Sensitive Data.This issue affects My Tickets: from n/a through <= 2.1.0.	7.5	More Details
CVE-	Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow		

2026-27142	XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.	7.5	More Details
CVE-2026-23662	Missing authentication for critical function in Azure IoT Explorer allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2025-69340	Missing Authorization vulnerability in BuddhaThemes WeDesignTech Ultimate Booking Addon wedesigntech-ultimate-booking-addon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WeDesignTech Ultimate Booking Addon: from n/a through <= 1.0.3.	7.5	More Details
CVE-2025-15576	If two sibling jails are restricted to separate filesystem trees, which is to say that neither of the two jail root directories is an ancestor of the other, jailed processes may nonetheless be able to access a shared directory via a nullfs mount, if the administrator has configured one. In this case, cooperating processes in the two jails may establish a connection using a unix domain socket and exchange directory descriptors with each other. When performing a filesystem name lookup, at each step of the lookup, the kernel checks whether the lookup would descend below the jail root of the current process. If the jail root directory is not encountered, the lookup continues. In a configuration where processes in two different jails are able to exchange file descriptors using a unix domain socket, it is possible for a jailed process to receive a directory for a descriptor that is below that process' jail root. This enables full filesystem access for a jailed process, breaking the chroot. Note that the system administrator is still responsible for ensuring that an unprivileged user on the jail host is not able to pass directory descriptors to a jailed process, even in a patched kernel.	7.5	More Details
CVE-2026-3038	The rtsock_msg_buffer() function serializes routing information into a buffer. As a part of this, it copies sockaddr structures into a sockaddr_storage structure on the stack. It assumes that the source sockaddr length field had already been validated, but this is not necessarily the case, and it's possible for a malicious userspace program to craft a request which triggers a 127-byte overflow. In practice, this overflow immediately overwrites the canary for the rtsock_msg_buffer() stack frame, resulting in a panic once the function returns. The bug allows an unprivileged user to crash the kernel by triggering a stack buffer overflow in rtsock_msg_buffer(). In particular, the overflow will corrupt a stack canary value that is verified when the function returns; this mitigates the impact of the stack overflow by triggering a kernel panic. Other kernel bugs may exist which allow userspace to find the canary value and thus defeat the mitigation, at which point local privilege escalation may be possible.	7.5	More Details
CVE-2025-70238	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard52.	7.5	More Details
CVE-2025-70243	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard534.	7.5	More Details
CVE-2025-70250	Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formdumpeasysetup.	7.5	More Details
CVE-2025-70047	An issue pertaining to CWE-400: Uncontrolled Resource Consumption was discovered in Nexusoft NexusInterface v3.2.0-beta.2.	7.5	More Details
CVE-2026-3588	A server-side request forgery (SSRF) vulnerability in IKEA Dirigera v2.866.4 allows an attacker to exfiltrate private keys by sending a crafted request.	7.5	More Details
CVE-2026-28076	Missing Authorization vulnerability in Frenify Guff guff allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Guff: from n/a through <= 1.0.1.	7.5	More Details
CVE-2025-62166	FreshRSS is a free, self-hostable RSS aggregator. Prior 1.28.0, a bug in the auth logic related to master authentication tokens, this restriction is bypassed. Usually only the default user's feed should be viewable if anonymous viewing is enabled, and feeds of other users should be private. This vulnerability is fixed in 1.28.0.	7.5	More Details
CVE-2026-28691	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, an uninitialized pointer dereference vulnerability exists in the JBIG decoder due to a missing check. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	7.5	More Details

CVE-2026-29045	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.12.4, when using serveStatic together with route-based middleware protections (e.g. app.use('/admin/*', ...)), inconsistent URL decoding allowed protected static resources to be accessed without authorization. The router used decodeURI, while serveStatic used decodeURIComponent. This mismatch allowed paths containing encoded slashes (%2F) to bypass middleware protections while still resolving to the intended filesystem path. This issue has been patched in version 4.12.4.	7.5	More Details
CVE-2026-3585	The The Events Calendar plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 6.15.17 via the 'ajax_create_import' function. This makes it possible for authenticated attackers, with Author-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2025-56421	SQL Injection vulnerability in LimeSurvey before v.6.15.4+250710 allows a remote attacker to obtain sensitive information from the database.	7.5	More Details
CVE-2026-28435	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.35.0, cpp-httplib (httplib.h) does not enforce Server::set_payload_max_length() on the decompressed request body when using HandlerWithContentReader (streaming ContentReader) with Content-Encoding: gzip (or other supported encodings). A small compressed payload can expand beyond the configured payload limit and be processed by the application, enabling a payload size limit bypass and potential denial of service (CPU/memory exhaustion). This vulnerability is fixed in 0.35.0.	7.5	More Details
CVE-2026-31830	sigstore-ruby is a pure Ruby implementation of the sigstore verify command from the sigstore/cosign project. Prior to 0.2.3, Sigstore::Verifier#verify does not propagate the VerificationFailure returned by verify_in_toto when the artifact digest does not match the digest in the in-toto attestation subject. As a result, verification of DSSE bundles containing in-toto statements returns VerificationSuccess regardless of whether the artifact matches the attested subject. This vulnerability is fixed in 0.2.3.	7.5	More Details
CVE-2026-27778	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks by suppressing or mis-routing legitimate charger telemetry, or conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2025-14769	In some cases, the \`tcp-setmss\` handler may free the packet data and throw an error without halting the rule processing engine. A subsequent rule can then allow the traffic after the packet data is gone, resulting in a NULL pointer dereference. Maliciously crafted packets sent from a remote host may result in a Denial of Service (DoS) if the \`tcp-setmss\` directive is used and a subsequent rule would allow the traffic to pass.	7.5	More Details
CVE-2025-69411	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Robert Seyfriedsberger ionCube tester plus ioncube-tester-plus allows Path Traversal.This issue affects ionCube tester plus: from n/a through <= 1.3.	7.5	More Details
CVE-2025-69279	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-41772	An unauthenticated remote attacker can obtain valid session tokens because they are exposed in plaintext within the URL parameters of the wwwupdate.cgi endpoint in UBR.	7.5	More Details
CVE-2026-27388	Missing Authorization vulnerability in designthemes DesignThemes Booking Manager designthemes-booking-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DesignThemes Booking Manager: from n/a through <= 2.0.	7.5	More Details
CVE-2026-27386	Missing Authorization vulnerability in designthemes DesignThemes Directory Addon designthemes-directory-addon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DesignThemes Directory Addon: from n/a through <= 1.8.	7.5	More Details
CVE-2026-27374	Missing Authorization vulnerability in vanquish WooCommerce Order Details woocommerce-order-details allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Order Details: from n/a through <= 3.1.	7.5	More Details
CVE-2026-27370	Insertion of Sensitive Information Into Sent Data vulnerability in Premio Chaty chaty allows Retrieve Embedded Sensitive Data.This issue affects Chaty: from n/a through <= 3.5.1.	7.5	More Details
CVE-			More

2026-3631	Delta Electronics COMMGR2 has Buffer Over-read DoS vulnerability.	7.5	Details
CVE-2026-28039	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wpDataTables wpDataTables wpdatatables allows PHP Local File Inclusion.This issue affects wpDataTables: from n/a through <= 6.5.0.1.	7.5	More Details
CVE-2026-27361	Missing Authorization vulnerability in WebCodingPlace Responsive Posts Carousel Pro responsive-posts-carousel-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Responsive Posts Carousel Pro: from n/a through <= 15.1.	7.5	More Details
CVE-2025-61611	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed..	7.5	More Details
CVE-2025-69278	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-61612	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-61613	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-61614	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2026-24385	Deserialization of Untrusted Data vulnerability in gerritvanaaken Podlove Web Player podlove-web-player allows Object Injection.This issue affects Podlove Web Player: from n/a through <= 5.9.1.	7.5	More Details
CVE-2025-61615	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-61616	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2026-22479	Missing Authorization vulnerability in ThemeRuby Easy Post Submission easy-post-submission allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Post Submission: from n/a through <= 2.2.0.	7.5	More Details
CVE-2026-30244	Plane is an an open-source project management tool. Prior to version 1.2.2, unauthenticated attackers can enumerate workspace members and extract sensitive information including email addresses, user roles, and internal identifiers. The vulnerability stems from Django REST Framework permission classes being incorrectly configured to allow anonymous access to protected endpoints. This issue has been patched in version 1.2.2.	7.5	More Details
CVE-2026-23661	Cleartext transmission of sensitive information in Azure IoT Explorer allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-25181	Out-of-bounds read in Windows GDI+ allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-30910	Crypt::Sodium::XS versions through 0.001000 for Perl has potential integer overflows. Combined aead encryption, combined signature creation, and bin2hex functions do not check that output size will be less than SIZE_MAX, which could lead to integer wraparound causing an undersized output buffer. This can cause a crash in bin2hex and encryption algorithms other than aes256gcm. For aes256gcm encryption and signatures, an undersized buffer could lead to buffer overflow. Encountering this issue is unlikely as the message length would need to be very large. For bin2hex the input size would have to be > SIZE_MAX / 2 For aegis encryption the input size would need to be > SIZE_MAX - 32U For other encryption the input size would need to be > SIZE_MAX - 16U For signatures the input size would need to be > SIZE_MAX - 64U	7.5	More Details

CVE-2025-14353	The ZIP Code Based Content Protection plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 1.0.2 via the 'zipcode' parameter. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-2020	The JS Archive List plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 6.1.7 via the 'included' shortcode attribute. This is due to the deserialization of untrusted input supplied via the 'included' parameter of the plugin's shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.5	More Details
CVE-2026-28429	Talishar is a fan-made Flesh and Blood project. Prior to commit 6be3871, a Path Traversal vulnerability was identified in the gameName parameter. While the application's primary entry points implement input validation, the ParseGamestate.php component can be accessed directly as a standalone script. In this scenario, the absence of internal sanitization allows for directory traversal sequences (e.g., ../) to be processed, potentially leading to unauthorized file access. This issue has been patched in commit 6be3871.	7.5	More Details
CVE-2026-30827	express-rate-limit is a basic rate-limiting middleware for Express. In versions starting from 8.0.0 and prior to versions 8.0.2, 8.1.1, 8.2.2, and 8.3.0, the default keyGenerator in express-rate-limit applies IPv6 subnet masking (/56 by default) to all addresses that net.isIPv6() returns true for. This includes IPv4-mapped IPv6 addresses (::ffff:x.x.x.x), which Node.js returns as request.ip on dual-stack servers. Because the first 80 bits of all IPv4-mapped addresses are zero, a /56 (or any /32 to /80) subnet mask produces the same network key (::/56) for every IPv4 client. This collapses all IPv4 traffic into a single rate-limit bucket: one client exhausting the limit causes HTTP 429 for all other IPv4 clients. This issue has been patched in versions 8.0.2, 8.1.1, 8.2.2, and 8.3.0.	7.5	More Details
CVE-2026-24308	Improper handling of configuration values in ZKConfig in Apache ZooKeeper 3.8.5 and 3.9.4 on all platforms allows an attacker to expose sensitive information stored in client configuration in the client's logfile. Configuration values are exposed at INFO level logging rendering potential production systems affected by the issue. Users are recommended to upgrade to version 3.8.6 or 3.9.5 which fixes this issue.	7.5	More Details
CVE-2026-2219	It was discovered that dpkg-deb (a component of dpkg, the Debian package management system) does not properly validate the end of the data stream when uncompressing a zstd-compressed .deb archive, which may result in denial of service (infinite loop spinning the CPU).	7.5	More Details
CVE-2026-28696	Craft is a content management system (CMS). Prior to 4.17.0-beta.1 and 5.9.0-beta.1, the GraphQL directive @parseRefs, intended to parse internal reference tags (e.g., {user:1:email}), can be abused by both authenticated users and unauthenticated guests (if a Public Schema is enabled) to access sensitive attributes of any element in the CMS. The implementation in Elements::parseRefs fails to perform authorization checks, allowing attackers to read data they are not authorized to view. This vulnerability is fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	7.5	More Details
CVE-2026-3520	Multer is a node.js middleware for handling \`multipart/form-data\`. A vulnerability in Multer prior to version 2.1.1 allows an attacker to trigger a Denial of Service (DoS) by sending malformed requests, potentially causing stack overflow. Users should upgrade to version 2.1.1 to receive a patch. No known workarounds are available.	7.5	More Details
CVE-2026-1605	In Eclipse Jetty, versions 12.0.0-12.0.31 and 12.1.0-12.0.5, class GzipHandler exposes a vulnerability when a compressed HTTP request, with Content-Encoding: gzip, is processed and the corresponding response is not compressed. This happens because the JDK Inflater is allocated for decompressing the request, but it is not released because the release mechanism is tied to the compressed response. In this case, since the response is not compressed, the release mechanism does not trigger, causing the leak.	7.5	More Details
CVE-2026-29779	UptimeFlare is a serverless uptime monitoring & status page solution, powered by Cloudflare Workers. Prior to commit 377a596, configuration file uptime.config.ts exports both pageConfig (safe for client use) and workerConfig (server-only, contains sensitive data) from the same module. Due to pages/incidents.tsx importing and using workerConfig directly inside client-side component code, the entire workerConfig object was included in the client-side JavaScript bundle served to all visitors. This issue has been patched via commit 377a596.	7.5	More Details
CVE-2026-	Ghost is a Node.js content management system. From version 5.101.6 to 6.19.2, incomplete CSRF protections around /session/verify made it possible to use OTCs in login sessions different from the	7.5	More

29784	requesting session. In some scenarios this might have made it easier for phishers to take over a Ghost site. This issue has been patched in version 6.19.3.		Details
CVE-2026-30834	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. Prior to version 0.7.7, a Server-Side Request Forgery (SSRF) vulnerability in the /download endpoint allows any user with API access to induce the PinchTab server to make requests to arbitrary URLs, including internal network services and local system files, and exfiltrate the full response content. This issue has been patched in version 0.7.7.	7.5	More Details
CVE-2026-27603	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.4, the chart filter endpoint POST /project/:project_id/chart/:chart_id/filter is missing both verifyToken and checkPermissions middleware, allowing unauthenticated users to access chart data from any team/project. This issue has been patched in version 4.8.4.	7.5	More Details
CVE-2026-23674	Improper resolution of path equivalence in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	7.5	More Details
CVE-2026-23664	Improper restriction of communication channel to intended endpoints in Azure IoT Explorer allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-24281	Hostname verification in Apache ZooKeeper ZKTrustManager falls back to reverse DNS (PTR) when IP SAN validation fails, allowing attackers who control or spoof PTR records to impersonate ZooKeeper servers or clients with a valid certificate for the PTR name. It's important to note that attacker must present a certificate which is trusted by ZKTrustManager which makes the attack vector harder to exploit. Users are recommended to upgrade to version 3.8.6 or 3.9.5, which fixes this issue by introducing a new configuration option to disable reverse DNS lookup in client and quorum protocols.	7.4	More Details
CVE-2026-25569	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). An out-of-bounds write vulnerability exists in SICAM SIAPP SDK. This could allow an attacker to write data beyond the intended buffer, potentially leading to denial of service, or arbitrary code execution.	7.4	More Details
CVE-2026-25573	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). The affected application builds shell commands with caller-provided strings and executes them. An attacker could influence the executed command, potentially resulting in command injection and full system compromise.	7.4	More Details
CVE-2026-2713	IBM Trusteer Rapport installer 3.5.2309.290 IBM Trusteer Rapport could allow a local attacker to execute arbitrary code on the system, caused by DLL uncontrolled search path element vulnerability. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system.	7.4	More Details
CVE-2025-66413	Git for Windows is the Windows port of Git. Prior to 2.53.0(2), it is possible to obtain a user's NTLM hash by tricking them into cloning from a malicious server. Since NTLM hashing is weak, it is possible for the attacker to brute-force the user's account name and password. This vulnerability is fixed in 2.53.0(2).	7.4	More Details
CVE-2026-25570	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). The SICAM SIAPP SDK does not perform checks on input values potentially resulting in stack overflow. This could allow an attacker to perform code execution and denial of service.	7.4	More Details
CVE-2026-25167	Use after free in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2026-3758	A weakness has been identified in projectworlds Online Art Gallery Shop 1.0. Affected by this issue is some unknown functionality of the file /admin/adminHome.php. This manipulation of the argument Info causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-29082	Kestra is an event-driven orchestration platform. In versions from 1.1.10 and prior, Kestra’s execution-file preview renders user-supplied Markdown (.md) with markdown-it instantiated as html:true and injects the resulting HTML with Vue’s v-html without sanitisation. At time of publication, there are no publicly available patches.	7.3	More Details
CVE-2026-3744	A vulnerability has been found in code-projects Student Web Portal 1.0. This impacts the function valreg_passwdation of the file signup.php. The manipulation of the argument reg_passwd leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE-2026-3734	A flaw has been found in SourceCodester Client Database Management System 1.0. Affected is an unknown function of the file /fetch_manager_details.php of the component Endpoint. This manipulation of the argument manager_id causes improper authorization. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-3760	A vulnerability was detected in itsourcecode University Management System 1.0. This vulnerability affects unknown code of the file /view_result.php. Performing a manipulation of the argument seme results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-3759	A security vulnerability has been detected in projectworlds Online Art Gallery Shop 1.0. This affects an unknown part of the file /admin/adminHome.php. Such manipulation of the argument reach_nm leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-24912	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3794	A vulnerability was identified in doramart DoraCMS 3.0.x. This issue affects some unknown processing of the file /api/v1/mail/send of the component Email API. Such manipulation leads to improper authentication. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-3735	A vulnerability has been found in code-projects Simple Flight Ticket Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file SearchResultOneway.php. Such manipulation of the argument from leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-3757	A security flaw has been discovered in projectworlds Online Art Gallery Shop 1.0. Affected by this vulnerability is an unknown functionality of the file /?pass=1. The manipulation of the argument fnm results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-3746	A vulnerability was determined in SourceCodester Simple Responsive Tourism Website 1.0. Affected by this vulnerability is an unknown functionality of the file /tourism/classes/Login.php?f=login of the component Login. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-3747	A vulnerability was identified in itsourcecode University Management System 1.0. Affected by this issue is some unknown functionality of the file /add_result.php. Such manipulation of the argument subject leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-26194	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, there's a security issue in gogs where deleting a release can fail if a user controlled tag name is passed to git without the right separator, this lets git options get injected and mess with the process. This issue has been patched in version 0.14.2.	7.3	More Details
CVE-2026-27396	Missing Authorization vulnerability in e-plugins Directory Pro directory-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Directory Pro: from n/a through <= 2.5.6.	7.3	More Details
CVE-2026-26276	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, an attacker can store an HTML/JavaScript payload in a repository’s Milestone name, and when another user selects that Milestone on the New Issue page (/issues/new), a DOM-Based XSS is triggered. This issue has been patched in version 0.14.2.	7.3	More Details
CVE-2026-3736	A vulnerability was found in code-projects Simple Flight Ticket Booking System 1.0. Affected by this issue is some unknown functionality of the file SearchResultRoundtrip.php. Performing a manipulation of the argument from results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in		

CVE-2026-20748	predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-3764	A vulnerability was determined in SourceCodester Client Database Management System 1.0. The impacted element is an unknown function of the file /superadmin_user_update.php. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-3723	A security flaw has been discovered in code-projects Simple Flight Ticket Booking System 1.0. This affects an unknown function of the file /Admindelete.php. The manipulation of the argument flightno results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-28448	OpenClaw versions 2026.1.29 prior to 2026.2.1 contain a vulnerability in the Twitch plugin (must be installed and enabled) in which it fails to enforce the allowFrom allowlist when allowedRoles is unset or empty, allowing unauthorized Twitch users to trigger agent dispatch. Remote attackers can mention the bot in Twitch chat to bypass access control and invoke the agent pipeline, potentially causing unintended actions or resource exhaustion.	7.3	More Details
CVE-2026-2364	If a legitimate user confirms a self-update prompt or initiate an installation of a CODESYS Development System, a low privileged local attacker can gain elevated rights due to a TOCTOU vulnerability in the CODESYS installer.	7.3	More Details
CVE-2026-3709	A weakness has been identified in code-projects Simple Flight Ticket Booking System 1.0. This affects an unknown function of the file /register.php. Executing a manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-25702	A Improper Access Control vulnerability in the kernel of SUSE SUSE Linux Enterprise Server 12 SP5 breaks nftables, causing firewall rules applied via nftables to not be effective.This issue affects SUSE Linux Enterprise Server: from 9e6d9d4601768c75fdb0bad3fbbe636e748939c2 before 9c294edb7085fb91650bc12233495a8974c5ff2d.	7.3	More Details
CVE-2026-3762	A vulnerability has been found in SourceCodester Client Database Management System 1.0/3.1. Impacted is an unknown function of the file /superadmin_delete_manager.php of the component Endpoint. The manipulation of the argument manager_id leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-29023	Keygraph Shannon contains a hard-coded API key in its router configuration that, when the router component is enabled and exposed, allows network attackers to authenticate using the publicly known static key. An attacker able to reach the router port can proxy requests through the Shannon instance using the victim’s configured upstream provider API credentials, resulting in unauthorized API usage and potential disclosure of proxied request and response data. This vulnerability's general exploitability has been mitigated with the introduction of commit 023cc95.	7.3	More Details
CVE-2026-3708	A security flaw has been discovered in code-projects Simple Flight Ticket Booking System 1.0. The impacted element is an unknown function of the file /login.php. Performing a manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-3765	A vulnerability was identified in itsourcecode University Management System 1.0. This affects an unknown function of the file /att_single_view.php. Such manipulation of the argument dt leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-3730	A security flaw has been discovered in itsourcecode Free Hotel Reservation System 1.0. The affected element is an unknown function of the file /hotel/admin/mod_amenities/index.php?view=edit. Performing a manipulation of the argument amen_id/rmtype_id results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-27764	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers and enables session hijacking or shadowing, where the most recent connection displaces the legitimate charging station and receives backend commands intended for that station. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session	7.3	More Details

	requests.		
CVE-2026-3705	A vulnerability was found in code-projects Simple Flight Ticket Booking System 1.0. This issue affects some unknown processing of the file /Adminsearch.php. The manipulation of the argument flightno results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-3740	A weakness has been identified in itsourcecode University Management System 1.0. Impacted is an unknown function of the file /admin_search_student.php. This manipulation of the argument admin_search_student causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-3696	A vulnerability was found in Totolink N300RH 6..1c.1353_B20190305. The affected element is the function setWiFiWpsConfig of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-3693	A flaw has been found in Shy2593666979 AgentChat up to 2.3.0. This issue affects the function get_user_info/update_user_info of the file /src/backend/agentchat/api/v1/user.py of the component User Endpoint. This manipulation of the argument user_id causes improper control of resource identifiers. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-3818	A flaw has been found in Tiandy Easy7 CMS Windows 7.17.0. Impacted is an unknown function of the file /Easy7/apps/WebService/GetDBData.jsp. This manipulation of the argument strTBName causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-28542	Permission bypass vulnerability in the system service framework. Impact: Successful exploitation of this vulnerability may affect availability.	7.3	More Details
CVE-2026-25887	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.1, there is a remote code execution vulnerability via the MongoDB dataset Query. This issue has been patched in version 4.8.1.	7.2	More Details
CVE-2026-31834	Umbraco is an ASP.NET CMS. From 15.3.1 to before 16.5.1 and 17.2.2, A privilege escalation vulnerability has been identified in Umbraco CMS. Under certain conditions, authenticated backoffice users with permission to manage users, may be able to elevate their privileges due to insufficient authorization enforcement when modifying user group memberships. The affected functionality does not properly validate whether a user has sufficient privileges to assign highly privileged roles. This vulnerability is fixed in 16.5.1 and 17.2.2.	7.2	More Details
CVE-2026-1074	The WP App Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'app-bar-features' parameter in all versions up to, and including, 1.5. This is due to insufficient input sanitization and output escaping combined with a missing authorization check in the `App_Bar_Settings` class constructor. This makes it possible for unauthenticated attackers to inject arbitrary web scripts into multiple plugin settings that will execute whenever a user accesses the admin settings page.	7.2	More Details
CVE-2026-30958	OneUptime is a solution for monitoring and managing online services. Prior to 10.0.21, an unauthenticated path traversal in the /workflow/docs/:componentName endpoint allows reading arbitrary files from the server filesystem. The componentName route parameter is concatenated directly into a file path passed to res.sendFile() in orker/FeatureSet/Workflow/Index.ts with no sanitization or authentication middleware. This vulnerability is fixed in 10.0.21.	7.2	More Details
CVE-2026-2724	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form entry fields in all versions up to, and including, 2.0.5. This is due to insufficient input sanitization and output escaping on form submission data displayed in the admin Form Entries Trash view. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views the trashed form entries.	7.2	More Details
CVE-2026-29182	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.4 and 9.4.1-alpha.3, Parse Server's readOnlyMasterKey option allows access with master-level read privileges but is documented to deny all write operations. However, some endpoints incorrectly accept the readOnlyMasterKey for mutating operations. This allows a caller who only holds the readOnlyMasterKey to create, modify, and delete Cloud Hooks and to start Cloud Jobs, which can be used for data exfiltration. Any Parse Server deployment that uses the readOnlyMasterKey option is affected. Note than an attacker needs to know the readOnlyMasterKey to exploit this vulnerability. This issue has been patched in versions 8.6.4 and 9.4.1-alpha.3.	7.2	More Details

CVE-2026-3352	The Easy PHP Settings plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 1.0.4 via the `update_wp_memory_constants()` method. This is due to insufficient input validation on the `wp_memory_limit` and `wp_max_memory_limit` settings before writing them to `wp-config.php`. The `sanitize_text_field()` function used for sanitization does not filter single quotes, allowing an attacker to break out of the string context in a PHP `define()` statement. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject and execute arbitrary PHP code on the server by modifying `wp-config.php`, which is loaded on every page request.	7.2	More Details
CVE-2025-14675	The Meta Box plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'ajax_delete_file' function in all versions up to, and including, 5.11.1. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	7.2	More Details
CVE-2026-25836	An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox Cloud 5.0.4 may allow a privileged attacker with super-admin profile and CLI access to execute unauthorized code or commands via crafted HTTP requests.	7.2	More Details
CVE-2026-22572	An authentication bypass using an alternate path or channel vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.3, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2.2 through 7.2.11, FortiAnalyzer Cloud 7.6.0 through 7.6.3, FortiAnalyzer Cloud 7.4.0 through 7.4.7, FortiAnalyzer Cloud 7.2.2 through 7.2.10, FortiManager 7.6.0 through 7.6.3, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2.2 through 7.2.11, FortiManager Cloud 7.6.0 through 7.6.3, FortiManager Cloud 7.4.0 through 7.4.7, FortiManager Cloud 7.2.2 through 7.2.10 may allow an attacker with knowledge of the admins password to bypass multifactor authentication checks via submitting multiple crafted requests.	7.2	More Details
CVE-2026-1261	The MetForm Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Quiz feature in all versions up to, and including, 3.9.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-68648	A use of externally-controlled format string vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.7, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.7, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow an attacker to escalate its privileges via specially crafted requests.	7.2	More Details
CVE-2025-66178	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4.0 through 7.4.11, FortiWeb 7.2.0 through 7.2.12, FortiWeb 7.0.0 through 7.0.12 may allow an authenticated attacked to execute arbitrary commands via a specialy crafted HTTP request.	7.2	More Details
CVE-2025-14558	The rtsol(8) and rtsold(8) programs do not validate the domain search list options provided in router advertisement messages; the option body is passed to resolvconf(8) unmodified. resolvconf(8) is a shell script which does not validate its input. A lack of quoting meant that shell commands pass as input to resolvconf(8) may be executed.	7.2	More Details
CVE-2025-41767	A high-privileged remote attacker can fully compromise the device by abusing an update signature bypass vulnerability in the wwwupdate.cgi method in the web interface of UBR.	7.2	More Details
CVE-2026-3612	A vulnerability was determined in Wavlink WL-NU516U1 V240425. This affects the function sub_405AF4 of the file /cgi-bin/adm.cgi of the component OTA Online Upgrade. This manipulation of the argument firmware_url causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	7.2	More Details
CVE-2026-3613	A vulnerability was identified in Wavlink WL-NU516U1 V240425. This vulnerability affects the function sub_401A0C of the file /cgi-bin/login.cgi. Such manipulation of the argument ipaddr leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	7.2	More Details
CVE-2026-	The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites – PostX plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.0.8 via the `/ultp/v3/starter_dummy_post/` and `/ultp/v3/starter_import_content/` REST API endpoints. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web	7.2	More Details

1273	requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.		
CVE-2026-28695	Craft is a content management system (CMS). There is an authenticated admin RCE in Craft CMS 5.8.21 via Server-Side Template Injection using the create() Twig function combined with a Symfony Process gadget chain. The create() Twig function exposes Craft::createObject(), which allows instantiation of arbitrary PHP classes with constructor arguments. Combined with the bundled symfony/process dependency, this enables RCE. This bypasses the fix implemented for CVE-2025-57811 (patched in 5.8.7). This vulnerability is fixed in 5.9.0-beta.1 and 4.17.0-beta.1.	7.2	More Details
CVE-2026-20062	A vulnerability in the CLI of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software in multiple context mode could allow an authenticated, local attacker with administrative privileges in one context to copy files to or from another context, including configuration files. This vulnerability is due to improper access controls for Secure Copy Protocol (SCP) operations when the CiscoSSH stack is enabled. An attacker could exploit this vulnerability by authenticating to a non-admin context of the device and issuing crafted SCP copy commands in that non-admin context. A successful exploit could allow the attacker to read, create, or overwrite sensitive files that belong to another context, including the admin and system contexts. The attacker cannot directly impact the availability of services pertaining to other contexts. To exploit this vulnerability, the attacker must have valid administrative credentials for a non-admin context. Note: An attacker cannot list or enumerate files from another context and would need to know the exact file path, which increases the complexity of a successful attack.	7.2	More Details
CVE-2026-28784	Craft is a content management system (CMS). Prior to 5.8.22 and 4.16.18, it is possible to craft a malicious payload using the Twig map filter in text fields that accept Twig input under Settings in the Craft control panel or using the System Messages utility, which could lead to a RCE. For this to work, you must have administrator access to the Craft Control Panel, and allowAdminChanges must be enabled for this to work, which is against our recommendations for any non-dev environment. Alternatively, you can have a non-administrator account with allowAdminChanges disabled, but you have access to the System Messages utility. Users should update to the patched versions (5.8.22 and 4.16.18) to mitigate the issue.	7.2	More Details
CVE-2026-24963	Incorrect Privilege Assignment vulnerability in ameliabooking Amelia ameliabooking allows Privilege Escalation.This issue affects Amelia: from n/a through <= 1.2.38.	7.2	More Details
CVE-2026-28456	OpenClaw versions 2026.1.5 prior to 2026.2.14 contain a vulnerability in the Gateway in which it does not sufficiently constrain configured hook module paths before passing them to dynamic import(), allowing code execution. An attacker with gateway configuration modification access can load and execute unintended local modules in the Node.js process.	7.2	More Details
CVE-2025-59785	Improper validation of API end-point in 2N Access Commander version 3.4.2 and prior allows attacker to bypass password policy for backup file encryption. This vulnerability can only be exploited after authenticating with administrator privileges.	7.2	More Details
CVE-2025-59784	2N Access Commander version 3.4.1 and prior is vulnerable to log pollution. Certain parameters sent over API may be included in the logs without prior validation or sanitisation. This vulnerability can only be exploited after authenticating with administrator privileges.	7.2	More Details
CVE-2025-59783	API endpoint for user synchronization in 2N Access Commander version 3.4.1 did not have a sufficient input validation allowing for OS command injection. This vulnerability can only be exploited after authenticating with administrator privileges.	7.2	More Details
CVE-2026-28209	FreePBX is an open source IP PBX. From versions 16.0.17.2 to before 16.0.20 and from version 17.0.2.4 to before 17.0.5, a command injection vulnerability exists in FreePBX when using the ElevenLabs Text-to-Speech (TTS) engine in the recordings module. This issue has been patched in versions 16.0.20 and 17.0.5.	7.2	More Details
CVE-2026-2365	The Fluent Forms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `fluentform_step_form_save_data` AJAX action in all versions up to, and including, 6.1.17. This is due to the draft form submission endpoint being publicly accessible without authentication or nonce verification, combined with insufficient input sanitization and output escaping of form field data. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views a partial form entry.	7.2	More Details
CVE-2026-28436	Frappe is a full-stack web application framework. Prior to versions 16.11.0 and 15.102.0, an attacker can set a crafted image URL that results in XSS when the avatar is displayed, and it can be triggered for other users via website page comments. This issue has been patched in versions 16.11.0 and	7.2	More Details

	15.102.0.		
CVE-2026-1945	The WPBookit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpb_user_name' and 'wpb_user_email' parameters in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-3452	Concrete CMS below version 9.4.8 is vulnerable to Remote Code Execution by stored PHP object injection into the Express Entry List block via the columns parameter. An authenticated administrator can store attacker-controlled serialized data in block configuration fields that are later passed to unserialize() without class restrictions or integrity checks. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 8.9 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H. Thanks YJK (@YJK0805 https://hackerone.com/yjk0805) of ZUSO ART https://zuso.ai/ for reporting.	7.2	More Details
CVE-2026-28494	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a stack buffer overflow exists in ImageMagick's morphology kernel parsing functions. User-controlled kernel strings exceeding a buffer are copied into fixed-size stack buffers via memcpy without bounds checking, resulting in stack corruption. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	7.1	More Details
CVE-2026-28482	OpenClaw versions prior to 2026.2.12 construct transcript file paths using unsanitized sessionId parameters and sessionFile paths without enforcing directory containment. Authenticated attackers can exploit path traversal sequences like ../../etc/passwd in sessionId or sessionFile parameters to read or write arbitrary files outside the agent sessions directory.	7.1	More Details
CVE-2026-22465	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SeventhQueen BuddyApp buddyapp allows Reflected XSS.This issue affects BuddyApp: from n/a through <= 1.9.2.	7.1	More Details
CVE-2026-28112	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup AllInOne - Banner Rotator all-in-one-bannerRotator allows Reflected XSS.This issue affects AllInOne - Banner Rotator: from n/a through <= 3.8.	7.1	More Details
CVE-2026-28102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider Classic uberSlider_classic allows Reflected XSS.This issue affects UberSlider Classic: from n/a through <= 2.5.	7.1	More Details
CVE-2026-22455	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree Thebe thebe allows Reflected XSS.This issue affects Thebe: from n/a through <= 1.3.0.	7.1	More Details
CVE-2026-28110	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Playlist all-in-one-bannerWithPlaylist allows Reflected XSS.This issue affects LambertGroup - AllInOne - Banner with Playlist: from n/a through <= 3.8.	7.1	More Details
CVE-2026-28109	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Content Slider all-in-one-contentSlider allows Reflected XSS.This issue affects LambertGroup - AllInOne - Content Slider: from n/a through <= 3.8.	7.1	More Details
CVE-2026-28512	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to your services. From 2.0.0 to before 2.4.0, a flaw in callback URL validation allowed crafted redirect_uri values containing URL userinfo (@) to bypass legitimate callback pattern checks. If an attacker can trick a user into opening a malicious authorization link, the authorization code may be redirected to an attacker-controlled host. This vulnerability is fixed in 2.4.0.	7.1	More Details
CVE-2026-28459	OpenClaw versions prior to 2026.2.12 fail to validate the sessionFile path parameter, allowing authenticated gateway clients to write transcript data to arbitrary locations on the host filesystem. Attackers can supply a sessionFile path outside the sessions directory to create files and append data repeatedly, potentially causing configuration corruption or denial of service.	7.1	More Details
CVE-2026-22440	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree Thecs thecs allows Reflected XSS.This issue affects Thecs: from n/a through <= 1.4.7.	7.1	More Details
CVE-2026-22438	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree TheBi thebi allows Reflected XSS.This issue affects TheBi: from n/a through <= 1.0.5.	7.1	More Details

CVE-2026-28103	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LBG Zoominoutslider lbg_zoominoutslider allows Reflected XSS.This issue affects LBG Zoominoutslider: from n/a through <= 5.4.5.	7.1	More Details
CVE-2026-28281	InstantCMS is a free and open source content management system. Prior to 2.18.1, InstantCMS does not validate CSRF tokens, which allows attackers grant moderator privileges to users, execute scheduled tasks, move posts to trash, and accept friend requests on behalf of the user. This vulnerability is fixed in 2.18.1.	7.1	More Details
CVE-2026-30926	SiYuan is a personal knowledge management system. Prior to 3.5.10, a privilege escalation vulnerability exists in the publish service of SiYuan Note that allows low-privilege publish accounts (RoleReader) to modify notebook content via the /api/block/appendHeadingChildren API endpoint. The endpoint requires only the model.CheckAuth role, which accepts RoleReader sessions, but it does not enforce stricter checks, such as CheckAdminRole or CheckReadonly. This allows remote authenticated publish users with read-only privileges to append new blocks to existing documents, compromising the integrity of stored notes.	7.1	More Details
CVE-2018-25180	Maitra 1.7.2 contains an sql injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the mailid parameter in outmail and inmail modules. Attackers can also download the SQLite database file directly from the application directory to extract sensitive mail tracking data and credentials.	7.1	More Details
CVE-2026-25960	vLLM is an inference and serving engine for large language models (LLMs). The SSRF protection fix for CVE-2026-24779 add in 0.15.1 can be bypassed in the load_from_url_async method due to inconsistent URL parsing behavior between the validation layer and the actual HTTP client. The SSRF fix uses urllib3.util.parse_url() to validate and extract the hostname from user-provided URLs. However, load_from_url_async uses aiohttp for making the actual HTTP requests, and aiohttp internally uses the yarl library for URL parsing. This vulnerability in 0.17.0.	7.1	More Details
CVE-2026-28477	OpenClaw versions prior to 2026.2.14 contain an oauth state validation bypass vulnerability in the manual Chutes login flow that allows attackers to bypass CSRF protection. An attacker can convince a user to paste attacker-controlled OAuth callback data, enabling credential substitution and token persistence for unauthorized accounts.	7.1	More Details
CVE-2026-28108	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Thumbnails all-in-one-thumbnailsBanner allows Reflected XSS.This issue affects LambertGroup - AllInOne - Banner with Thumbnails: from n/a through <= 3.8.	7.1	More Details
CVE-2026-22467	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mwtemplates DeepDigital deepdigital allows Reflected XSS.This issue affects DeepDigital: from n/a through <= 1.0.2.	7.1	More Details
CVE-2018-25165	Galaxy Forces MMORPG 0.5.8 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'type' parameter. Attackers can send POST requests to ads.php with crafted SQL payloads in the type parameter to extract sensitive database information including usernames, databases, and version details.	7.1	More Details
CVE-2026-28101	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider MouseInteraction uberSlider_mouseinteraction allows Reflected XSS.This issue affects UberSlider MouseInteraction: from n/a through <= 2.3.	7.1	More Details
CVE-2026-28075	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in p-themes Porto porto allows Reflected XSS.This issue affects Porto: from n/a through <= 7.6.2.	7.1	More Details
CVE-2026-27541	Incorrect Privilege Assignment vulnerability in Josh Kohlbach Wholesale Suite woocommerce-wholesale-prices allows Privilege Escalation.This issue affects Wholesale Suite: from n/a through <= 2.2.6.	7.1	More Details
CVE-2026-27385	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes DesignThemes Portfolio designthemes-portfolio allows Reflected XSS.This issue affects DesignThemes Portfolio: from n/a through <= 1.3.	7.1	More Details
CVE-2026-27382	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RadiusTheme Metro metro allows DOM-Based XSS.This issue affects Metro: from n/a through <= 2.13.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in		

2026-27376	JanStudio Claue - Clean, Minimal Elementor WooCommerce Theme claue allows Reflected XSS.This issue affects Claue - Clean, Minimal Elementor WooCommerce Theme: from n/a through <= 2.2.7.	7.1	More Details
CVE-2026-27375	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JanStudio Gecko gecko allows Reflected XSS.This issue affects Gecko: from n/a through <= 1.9.8.	7.1	More Details
CVE-2026-27367	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Musico musico allows Reflected XSS.This issue affects Musico: from n/a through <= 3.2.4.	7.1	More Details
CVE-2026-27363	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kamleshyadav WP Bakery Autoresponder Addon vc-autoresponder-addon allows Stored XSS.This issue affects WP Bakery Autoresponder Addon: from n/a through <= 1.0.6.	7.1	More Details
CVE-2026-28042	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify Listify listify allows Reflected XSS.This issue affects Listify: from n/a through <= 3.2.5.	7.1	More Details
CVE-2026-28072	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PixFort pixfort Core pixfort-core allows Reflected XSS.This issue affects pixfort Core: from n/a through <= 3.2.22.	7.1	More Details
CVE-2026-27359	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fox-themes Awa Plugins awa-plugins allows Reflected XSS.This issue affects Awa Plugins: from n/a through <= 1.4.4.	7.1	More Details
CVE-2026-28100	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider PerpetuumMobile uberSlider_perpetuummobile allows Reflected XSS.This issue affects UberSlider PerpetuumMobile: from n/a through <= 2.3.	7.1	More Details
CVE-2026-27358	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Architecturer architecturer allows Reflected XSS.This issue affects Architecturer: from n/a through <= 3.8.8.	7.1	More Details
CVE-2026-28099	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider Ultra uberSlider_ultra allows Reflected XSS.This issue affects UberSlider Ultra: from n/a through <= 2.3.	7.1	More Details
CVE-2018-25191	Facturation System 1.0 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'mod_id' parameter. Attackers can send POST requests to the editar_producto.php endpoint with crafted SQL payloads in the mod_id parameter to extract sensitive database information including usernames, database names, and version details.	7.1	More Details
CVE-2026-27353	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand News grandnews allows Reflected XSS.This issue affects Grand News: from n/a through <= 3.4.3.	7.1	More Details
CVE-2026-29077	Frappe is a full-stack web application framework. Prior to versions 15.98.0 and 14.100.0, due to a lack of validation when sharing documents, a user could share a document with a permission that they themselves didn't have. This issue has been patched in versions 15.98.0 and 14.100.0.	7.1	More Details
CVE-2026-27352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Starto starto allows Reflected XSS.This issue affects Starto: from n/a through <= 2.1.9.	7.1	More Details
CVE-2026-27348	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Photography photography allows DOM-Based XSS.This issue affects Photography: from n/a through <= 7.6.1.	7.1	More Details
CVE-2026-27332	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Agrofood agrofood allows Reflected XSS.This issue affects Agrofood: from n/a through <= 1.3.0.	7.1	More Details
CVE-2026-28126	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sizam RH Frontend Publishing Pro rh-frontend allows Reflected XSS.This issue affects RH Frontend Publishing Pro: from n/a through <= 4.3.2.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in		More

2026-28113	azzaroco Ultimate Learning Pro indeed-learning-pro allows Reflected XSS.This issue affects Ultimate Learning Pro: from n/a through <= 3.9.1.	7.1	Details
CVE-2026-28122	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro listingpro-plugin allows Reflected XSS.This issue affects ListingPro: from n/a through <= 2.9.8.	7.1	More Details
CVE-2026-28130	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AndonDesign UDesign u-design allows Reflected XSS.This issue affects UDesign: from n/a through <= 4.14.0.	7.1	More Details
CVE-2026-28127	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Lawyer Directory lawyer-directory allows Reflected XSS.This issue affects Lawyer Directory: from n/a through <= 1.3.2.	7.1	More Details
CVE-2026-31829	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.0.13, Flowise exposes an HTTP Node in AgentFlow and Chatflow that performs server-side HTTP requests using user-controlled URLs. By default, there are no restrictions on target hosts, including private/internal IP ranges (RFC 1918), localhost, or cloud metadata endpoints. This enables Server-Side Request Forgery (SSRF), allowing any user interacting with a publicly exposed chatflow to force the Flowise server to make requests to internal network resources that are inaccessible from the public internet. This vulnerability is fixed in 3.0.13.	7.1	More Details
CVE-2026-29778	pyLoad is a free and open-source download manager written in Python. From version 0.5.0b3.dev13 to 0.5.0b3.dev96, the edit_package() function implements insufficient sanitization for the pack_folder parameter. The current protection relies on a single-pass string replacement of "../", which can be bypassed using crafted recursive traversal sequences. This issue has been patched in version 0.5.0b3.dev97.	7.1	More Details
CVE-2026-28548	Vulnerability of improper verification in the email application. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.1	More Details
CVE-2026-30945	StudioCMS is a server-side-rendered, Astro native, headless content management system. Prior to 0.4.0, the DELETE /studiocms_api/dashboard/api-tokens endpoint allows any authenticated user with editor privileges or above to revoke API tokens belonging to any other user, including admin and owner accounts. The handler accepts tokenID and userID directly from the request payload without verifying token ownership, caller identity, or role hierarchy. This enables targeted denial of service against critical integrations and automations. This vulnerability is fixed in 0.4.0.	7.1	More Details
CVE-2019-25503	PHPads 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the bannerID parameter in click.php3. Attackers can submit crafted bannerID values using SQL comment syntax and functions like extractvalue to extract sensitive database information such as the current database name.	7.1	More Details
CVE-2019-25505	Tradebox 5.4 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the symbol parameter. Attackers can send POST requests to the monthly_deposit endpoint with malicious symbol values using boolean-based blind, time-based blind, error-based, or union-based SQL injection techniques to extract sensitive database information.	7.1	More Details
CVE-2026-28137	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuanticaLabs MediCenter - Health Medical Clinic medicenter allows Reflected XSS.This issue affects MediCenter - Health Medical Clinic: from n/a through <= 14.9.	7.1	More Details
CVE-2026-28037	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ashanjay EventON eventon allows Reflected XSS.This issue affects EventON: from n/a through <= 4.9.12.	7.1	More Details
CVE-2026-23668	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-25170	Use after free in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	7.0	More Details

24285			
CVE-2026-23667	Use after free in Broadcast DVR allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-25179	Improper validation of specified type of input in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-25178	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-24295	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Device Association Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-23671	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Bluetooth RFCOM Protocol Driver allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-3787	A weakness has been identified in UltraVNC 1.6.4.0 on Windows. This affects an unknown function in the library cryptbase.dll of the component Windows Service. This manipulation causes uncontrolled search path. The attack requires local access. A high degree of complexity is needed for the attack. The exploitability is reported as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-24296	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Device Association Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-25171	Use after free in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-68482	A improper certificate validation vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.8, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer 6.4 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.8, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager 6.4 all versions may allow a remote unauthenticated attacker to view confidential information via a man in the middle [MiTM] attack.	6.9	More Details
CVE-2026-28690	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a stack buffer overflow vulnerability exists in the MNG encoder. There is a bounds checks missing that could corrupting the stack with attacker-controlled data. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	6.9	More Details
CVE-2025-62879	A vulnerability has been identified within the Rancher Backup Operator, resulting in the leakage of S3 tokens (both accessKey and secretKey) into the rancher-backup-operator pod's logs.	6.8	More Details
CVE-2026-28277	LangGraph SQLite Checkpoint is an implementation of LangGraph CheckpointSaver that uses SQLite DB (both sync and async, via aiosqlite). In version 1.0.9 and prior, LangGraph checkpointers can load msgpack-encoded checkpoints that reconstruct Python objects during deserialization. If an attacker can modify checkpoint data in the backing store (for example, after a database compromise or other privileged write access to the persistence layer), they can potentially supply a crafted payload that triggers unsafe object reconstruction when the checkpoint is loaded. No known patch is public.	6.8	More Details
CVE-2026-20025	A vulnerability in the OSPF protocol of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an authenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. To exploit this vulnerability, the attacker must have the OSPF secret key. This vulnerability is due to insufficient input validation when processing OSPF link-state update (LSU) packets. An attacker could exploit this vulnerability by sending crafted OSPF LSU packets. A successful exploit could allow the attacker to corrupt the heap, causing the device to reload, resulting in a DoS condition.	6.8	More Details
CVE-	Concrete CMS below version 9.4.8 is subject to CSRF by a Rogue Administrator using the Anti-Spam Allowlist Group Configuration via group_id parameter which can leads to a security bypass since		More

2026-2994	changes are saved prior to checking the CSRF token. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks z3rco for reporting	6.8	Details
CVE-2026-28547	Vulnerability of uninitialized pointer access in the scanning module. Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2026-20024	A vulnerability in the OSPF protocol of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an authenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. To exploit this vulnerability, the attacker must have the OSPF secret key. This vulnerability is due to heap corruption in OSPF when parsing packets. An attacker could exploit this vulnerability by sending crafted packets to the OSPF service. A successful exploit could allow the attacker to corrupt the heap, causing the affected device to reload, resulting in a DoS condition.	6.8	More Details
CVE-2026-20020	A vulnerability in the OSPF protocol of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. If OSPF authentication is enabled, the attacker must know the secret key to exploit this vulnerability. This vulnerability is due to insufficient input validation when processing OSPF update packets. An attacker could exploit this vulnerability by sending crafted OSPF update packets. A successful exploit could allow the attacker to create a buffer overflow, causing the affected device to reload, resulting in a DoS condition.	6.8	More Details
CVE-2026-30931	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16, a heap-based buffer overflow in the UHDR encoder can happen due to truncation of a value and it would allow an out of bounds write. This vulnerability is fixed in 7.1.2-16.	6.8	More Details
CVE-2026-28450	OpenClaw versions prior to 2026.2.12 with the optional Nostr plugin enabled expose unauthenticated HTTP endpoints at /api/channels/nostr/:accountId/profile and /api/channels/nostr/:accountId/profile/import that allow reading and modifying Nostr profiles without gateway authentication. Remote attackers can exploit these endpoints to read sensitive profile data, modify Nostr profiles, persist malicious changes to gateway configuration, and publish signed Nostr events using the bot's private key when the gateway HTTP port is accessible beyond localhost.	6.8	More Details
CVE-2026-20050	A vulnerability in the Do Not Decrypt exclusion feature of the SSL decryption feature of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management during the inspection of TLS 1.2 encrypted traffic. An attacker could exploit this vulnerability by sending crafted TLS 1.2 encrypted traffic through an affected device. A successful exploit could allow the attacker to cause a reload of an affected device. Note: This vulnerability only affects traffic that is encrypted by TLS 1.2. Other versions of TLS are not affected.	6.8	More Details
CVE-2026-28686	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, A heap-buffer-overflow vulnerability exists in the PCL encode due to an undersized output buffer allocation. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	6.8	More Details
CVE-2026-30937	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a 32-bit unsigned integer overflow in the XWD (X Windows) encoder can cause an undersized heap buffer allocation. When writing a extremely large image an out of bounds heap write can occur. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	6.8	More Details
CVE-2026-24288	Heap-based buffer overflow in Windows Mobile Broadband allows an unauthorized attacker to execute code with a physical attack.	6.8	More Details
CVE-2026-21424	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	6.7	More Details
CVE-2026-25605	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). The affected application performs file deletion without properly validating the file path or target. An attacker could delete files or sockets that the affected process has permission to remove, potentially resulting in denial of service or service disruption.	6.7	More Details
CVE-2026-26124	'.../...//' in Azure Compute Gallery allows an authorized attacker to elevate privileges locally.	6.7	More Details
	Umbraco is an ASP.NET CMS. From 16.2.0 to before 16.5.1 and 17.2.2, An authenticated backoffice		

CVE-2026-31833	user with access to Settings can inject malicious HTML into property type descriptions. Due to an overly permissive attributeNameCheck configuration (/.+/) in the UFM DOMPurify instance, event handler attributes such as onclick and onload, when used within Umbraco web components (umb-*, uui-*, ufm-*) were not filtered. This vulnerability is fixed in 16.5.1 and 17.2.2.	6.7	More Details
CVE-2026-21421	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	6.7	More Details
CVE-2025-48418	A hidden functionality vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.3, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2.0 through 7.2.10, FortiAnalyzer 7.0.0 through 7.0.14, FortiAnalyzer 6.4 all versions, FortiAnalyzer Cloud 7.6.2, FortiAnalyzer Cloud 7.4.1 through 7.4.7, FortiAnalyzer Cloud 7.2.1 through 7.2.10, FortiAnalyzer Cloud 7.0.1 through 7.0.14, FortiAnalyzer Cloud 6.4 all versions, FortiManager 7.6.0 through 7.6.3, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2.0 through 7.2.10, FortiManager 7.0.0 through 7.0.14, FortiManager 6.4 all versions, FortiManager Cloud 7.6.2 through 7.6.3, FortiManager Cloud 7.4.1 through 7.4.7, FortiManager Cloud 7.2.1 through 7.2.10, FortiManager Cloud 7.0.1 through 7.0.14, FortiManager Cloud 6.4 all versions may allow a remote authenticated read-only admin with CLI access to escalate their privilege via use of a hidden command.	6.7	More Details
CVE-2026-21423	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect default permissions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to code execution, denial of service, elevation of privileges, and information disclosure.	6.7	More Details
CVE-2026-23651	Permissive regular expression in Azure Compute Gallery allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2026-22270	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an uncontrolled search path element vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.	6.7	More Details
CVE-2026-21426	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.	6.7	More Details
CVE-2026-21425	Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	6.7	More Details
CVE-2025-70342	erase-install prior to v40.4 commit 2c31239 writes swiftDialog credential output to a hardcoded path /var/tmp/dialog.json. This allows an unauthenticated attacker to intercept admin credentials entered during reinstall/erase operations via creating a named pipe.	6.6	More Details
CVE-2026-28801	Natro Macro is an open-source Bee Swarm Simulator macro written in AutoHotkey. Prior to version 1.1.0, any ahk code contained inside of a pattern or path file is executed by the macro. Since users commonly share path/pattern files, an attacker could share a file containing malicious code, which is then executed by the program. This code can operate in silence alongside the pattern, running in the background to do whatever the attacker pleases. This issue has been patched in version 1.1.0.	6.6	More Details
CVE-2026-30897	A stack-based buffer overflow vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow a remote authenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands via crafted HTTP requests.	6.6	More Details
CVE-2026-24640	A Stack-based Buffer Overflow vulnerability [CWE-121] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0.2 through 7.0.12 may allow a remote authenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands via crafted HTTP requests.	6.6	More Details
CVE-2026-28549	Race condition vulnerability in the permission management service. Impact: Successful exploitation of this vulnerability may affect availability.	6.6	More Details
CVE-2026-	EC-CUBE provided by EC-CUBE CO.,LTD. contains a multi-factor authentication (MFA) bypass vulnerability. An attacker who has obtained a valid administrator ID and password may be able to	6.5	More Details

30777	bypass two-factor authentication and gain unauthorized access to the administrative page.		
CVE-2026-2893	The Page and Post Clone plugin for WordPress is vulnerable to SQL Injection via the 'meta_key' parameter in the content_clone() function in all versions up to, and including, 6.3. This is due to insufficient escaping on the user-supplied meta_key value and insufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The injection is second-order: the malicious payload is stored as a post meta key and executed when the post is cloned.	6.5	More Details
CVE-2026-30858	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.3.0, a DNS rebinding vulnerability in the web_fetch tool allows an unauthenticated attacker to bypass URL validation and access internal resources on the server, including private IP addresses (e.g., 127.0.0.1, 192.168.x.x). By crafting a malicious domain that resolves to a public IP during validation and subsequently resolves to a private IP during execution, an attacker can access sensitive local services and potentially exfiltrate data. This issue has been patched in version 0.3.0.	6.5	More Details
CVE-2026-28552	Out-of-bounds write vulnerability in the IMS module. Impact: Successful exploitation of this vulnerability may affect availability.	6.5	More Details
CVE-2026-3695	A vulnerability has been found in SourceCodester Modern Image Gallery App 1.0. Impacted is an unknown function of the file /delete.php. Such manipulation of the argument filename leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.5	More Details
CVE-2026-28104	Missing Authorization vulnerability in Aryan Shirani Bid Abadi Site Suggest site-suggest allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Site Suggest: from n/a through <= 1.3.9.	6.5	More Details
CVE-2026-28038	Missing Authorization vulnerability in Brainstorm_Force Ultimate Addons for WPBakery Page Builder ultimate_vc_addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Addons for WPBakery Page Builder: from n/a through <= 3.21.1.	6.5	More Details
CVE-2025-69343	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress theatre allows Stored XSS.This issue affects Theater for WordPress: from n/a through <= 0.19.	6.5	More Details
CVE-2026-3822	Taipower APP developed by Taipower has an Improper Certificate Validation vulnerability. When establishing an HTTPS connection with the server, the application fails to verify the server-side TLS/SSL certificate. This flaw allows an unauthenticated remote attackers to exploit the vulnerability to perform a Man-in-the-Middle (MITM) attack to read and tamper with network packets.	6.5	More Details
CVE-2026-3125	A Server-Side Request Forgery (SSRF) vulnerability was identified in the @opennextjs/cloudflare package, resulting from a path normalization bypass in the /cdn-cgi/image/ handler.The @opennextjs/cloudflare worker template includes a /cdn-cgi/image/ handler intended for development use only. In production, Cloudflare's edge intercepts /cdn-cgi/image/ requests before they reach the Worker. However, by substituting a backslash for a forward slash (/cdn-cgi\image/ instead of /cdn-cgi/image/), an attacker can bypass edge interception and have the request reach the Worker directly. The JavaScript URL class then normalizes the backslash to a forward slash, causing the request to match the handler and trigger an unvalidated fetch of arbitrary remote URLs. For example: https://victim-site.com/cdn-cgi\image/aaaa/https://attacker.com In this example, attacker-controlled content from attacker.com is served through the victim site's domain (victim-site.com), violating the same-origin policy and potentially misleading users or other services. Note: This bypass only works via HTTP clients that preserve backslashes in paths (e.g., curl --path-as-is). Browsers normalize backslashes to forward slashes before sending requests. Additionally, Cloudflare Workers with Assets and Cloudflare Pages suffer from a similar vulnerability. Assets stored under /cdn-cgi/ paths are not publicly accessible under normal conditions. However, using the same backslash bypass (/cdn-cgi\... instead of /cdn-cgi/...), these assets become publicly accessible. This could be used to retrieve private data. For example, Open Next projects store incremental cache data under /cdn-cgi/_next_cache, which could be exposed via this bypass.	6.5	More Details
CVE-2026-28769	A path traversal vulnerability exists in the /IDC_Logging/checkifdone.cgi script in International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver Web management portal version 101. An authenticated attacker can manipulate the `file` parameter to traverse directories and enumerate arbitrary files on the underlying filesystem. Due to the insecure perl file path handling function in use, a authenticated actor is able to preform directory traversal, with the backup endpoint confirming a file exists by indicating that a backup operation was successful or when using the path of	6.5	More Details

	a non existent file, the returned status is failed.		
CVE-2026-2363	The WP-Members Membership Plugin plugin for WordPress is vulnerable to SQL Injection via the 'order_by' attribute of the [wpmem_user_membership_posts] shortcode in all versions up to, and including, 3.5.5.1. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-1674	The Gutena Forms – Contact Form, Survey Form, Feedback Form, Booking Form, and Custom Form Builder plugin for WordPress is vulnerable to unauthorized modification of data due to missing authorization within the save_gutena_forms_schema() function in all versions up to, and including, 1.6.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to update option values to a structured array value on the WordPress site. This can be leveraged to update an option that would create an error on the site and deny service to legitimate users or be used to set some values, that would, for example enable site user registration when it is explicitly disabled.	6.5	More Details
CVE-2026-3846	Same-origin policy bypass in the CSS Parsing and Computation component. This vulnerability affects Firefox < 148.0.2.	6.5	More Details
CVE-2025-40896	The server certificate was not verified when an Arc agent connected to a Guardian or CMC. A malicious actor could perform a man-in-the-middle attack and intercept the communication between the Arc agent and the Guardian or CMC. This could result in theft of the client token and sensitive information (such as assets and alerts), impersonation of the server, or injection of spoofed data (such as false asset information or vulnerabilities) into the Guardian or CMC.	6.5	More Details
CVE-2026-30973	Appium is an automation framework that provides WebDriver-based automation possibilities for a wide range platforms. Prior to 7.0.6, @appium/support contains a ZIP extraction implementation (extractAllTo() via ZipExtractor.extract()) with a path traversal (Zip Slip) check that is non-functional. The check at line 88 of packages/support/lib/zip.js creates an Error object but never throws it, allowing malicious ZIP entries with ../ path components to write files outside the intended destination directory. This affects all JS-based extractions (the default code path), not only those using the fileNamesEncoding option. This vulnerability is fixed in 7.0.6.	6.5	More Details
CVE-2025-12801	A vulnerability was recently discovered in the rpc.mountd daemon in the nfs-utils package for Linux, that allows a NFSv3 client to escalate the privileges assigned to it in the /etc/exports file at mount time. In particular, it allows the client to access any subdirectory or subtree of an exported directory, regardless of the set file permissions, and regardless of any 'root_squash' or 'all_squash' attributes that would normally be expected to apply to that client.	6.5	More Details
CVE-2025-59787	2N Access Commander application version 3.4.2 and prior returns HTTP 500 Internal Server Error responses when receiving malformed or manipulated requests, indicating improper handling of invalid input and potential security or availability impacts.	6.5	More Details
CVE-2026-28781	Craft is a content management system (CMS). Prior to 4.17.0-beta.1 and 5.9.0-beta.1, the entry creation process allows for Mass Assignment of the authorId attribute. A user with "Create Entries" permission can inject the authorIds[] (or authorId) parameter into the POST request, which the backend processes without verifying if the current user is authorized to assign authorship to others. Normally, this field is not present in the request for users without the necessary permissions. By manually adding this parameter, an attacker can attribute the new entry to any user, including Admins. This effectively "spoofs" the authorship. This vulnerability is fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	6.5	More Details
CVE-2026-20001	A vulnerability in the REST API of Cisco Secure FMC Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to inadequate validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted requests to an affected device. A successful exploit could allow the attacker to obtain read access to the database and read certain files on the underlying operating system. To exploit this vulnerability, the attacker would need valid user credentials with any of the following roles: Administrator Security approver Access admin Network admin	6.5	More Details
CVE-2026-25689	An improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiDeceptor 6.2.0, FortiDeceptor 6.0 all versions, FortiDeceptor 5.3 all versions, FortiDeceptor 5.2 all versions, FortiDeceptor 5.1 all versions, FortiDeceptor 5.0 all versions, FortiDeceptor 4.3 all versions, FortiDeceptor 4.2 all versions, FortiDeceptor 4.1 all versions, FortiDeceptor 4.0 all versions may allow a privileged attacker with super-admin profile and CLI access to delete sensitive files via crafted HTTP requests.	6.5	More Details

CVE-2026-24297	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kerberos allows an unauthorized attacker to bypass a security feature over a network.	6.5	More Details
CVE-2026-20064	A vulnerability in of Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to cause the device to unexpectedly reload, causing a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied input. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the CLI prompt. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	6.5	More Details
CVE-2025-41712	An unauthenticated remote attacker who tricks a user to upload a manipulated HTML file can get access to sensitive information on the device. This is a result of incorrect permission assignment for the web server.	6.5	More Details
CVE-2025-41754	A low-privileged remote attacker can exploit the ubr-editfile method in wwwubr.cgi, an undocumented and unused API endpoint to read arbitrary files on the system.	6.5	More Details
CVE-2025-41710	An unauthenticated remote attacker may use hardcodes credentials to get access to the previously activated FTP Server with limited read and write privileges.	6.5	More Details
CVE-2026-30870	PowerSync Service is the server-side component of the PowerSync sync engine. In version 1.20.0, when using new sync streams with config.edition: 3, certain subquery filters were ignored when determining which data to sync to users. Depending on the sync stream configuration, this could result in authenticated users syncing data that should have been restricted. Only queries that gate synchronization using subqueries without partitioning the result set are affected. This vulnerability is fixed in 1.20.1.	6.5	More Details
CVE-2026-29085	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.12.4, when using streamSSE() in Streaming Helper, the event, id, and retry fields were not validated for carriage return (\r) or newline (\n) characters. Because the SSE protocol uses line breaks as field delimiters, this could allow injection of additional SSE fields within the same event frame if untrusted input was passed into these fields. This issue has been patched in version 4.12.4.	6.5	More Details
CVE-2025-7375	A denial-of-service (DoS) vulnerability was identified in Omada EAP610 v3. An attacker with adjacent network access can send crafted requests to cause the device's HTTP service to crash. This results in temporary service unavailability until the device is rebooted. This issue affects Omada EAP610 firmware versions prior to 1.6.0.	6.5	More Details
CVE-2026-28493	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16, an integer overflow vulnerability exists in the SIXEL decoer. The vulnerability allows an attacker to perform an out of bounds via a specially crafted image. This vulnerability is fixed in 7.1.2-16.	6.5	More Details
CVE-2026-2899	The Fluent Forms Pro Add On Pack plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.1.17. This is due to the `deleteFile()` method in the `Uploader` class lacking nonce verification and capability checks. The AJAX action is registered via `addPublicAjaxAction()` which creates both `wp_ajax_` and `wp_ajax_nopriv_` hooks. This makes it possible for unauthenticated attackers to delete arbitrary WordPress media attachments via the `attachment_id` parameter. Note: The researcher described file deletion via the `path` parameter using `sanitize_file_name()`, but the actual code uses `Protector::decrypt()` for path-based deletion which prevents exploitation. The vulnerability is exploitable via the `attachment_id` parameter instead.	6.5	More Details
CVE-2026-22459	Missing Authorization vulnerability in Blend Media WordPress CTA easy-sticky-sidebar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WordPress CTA: from n/a through <= 1.7.4.	6.5	More Details
CVE-2026-23546	Insertion of Sensitive Information Into Sent Data vulnerability in RadiusTheme Classified Listing classified-listing allows Retrieve Embedded Sensitive Data.This issue affects Classified Listing: from n/a through <= 5.3.4.	6.5	More Details
CVE-2026-23799	Missing Authorization vulnerability in Themeum Tutor LMS tutor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through <= 3.9.5.	6.5	More Details
CVE-2025-	A low-privileged remote attacker can directly interact with the wwwdnload.cgi endpoint to download	6.5	More

41763	any resource available to administrators, including system backups and certificate request files.		Details
CVE-2026-27354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace WooCommerce Coming Soon Product with Countdown woo-coming-soon-product allows Stored XSS.This issue affects WooCommerce Coming Soon Product with Countdown: from n/a through <= 5.0.	6.5	More Details
CVE-2026-27362	Missing Authorization vulnerability in kamleshyadav WP Bakery Autoresponder Addon vc-autoresponder-addon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Bakery Autoresponder Addon: from n/a through <= 1.0.6.	6.5	More Details
CVE-2025-41755	A low-privileged remote attacker can exploit the ubr-logread method in wwwubr.cgi to read arbitrary files on the system. The endpoint accepts a parameter specifying the log file to open (e.g., /tmp/weblog{some_number}), but this parameter is not properly validated, allowing an attacker to modify it to reference any file and retrieve its contents.	6.5	More Details
CVE-2026-30233	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.11.1, an authorization flaw in OliveTin allows authenticated users with view: false permission to enumerate action bindings and metadata via dashboard and API endpoints. Although execution (exec) may be correctly denied, the backend does not enforce IsAllowedView() when constructing dashboard and action binding responses. As a result, restricted users can retrieve action titles, IDs, icons, and argument metadata. This issue has been patched in version 3000.11.1.	6.5	More Details
CVE-2026-27777	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-25962	MarkUs is a web application for the submission and grading of student assignments. Prior to version 2.9.4, MarkUs currently extracts zip files without any size or entry-count limits. For example, instructors can upload a zip file to provide an assignment configuration; students can upload a zip file for an assignment submission and indicate its contents should be extracted. This issue has been patched in version 2.9.4.	6.5	More Details
CVE-2026-26122	Initialization of a resource with an insecure default in Azure Compute Gallery allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-1651	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'workflow_ids' parameter in all versions up to, and including, 5.9.16 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-27027	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-28492	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Prior to version 2.61.0, when a user creates a public share link for a directory, the withHashFile middleware in http/public.go uses filepath.Dir(link.Path) to compute the BasePathFs root. This sets the filesystem root to the parent directory instead of the shared directory itself, allowing anyone with the share link to browse and download files from all sibling directories. This issue has been patched in version 2.61.0.	6.5	More Details
CVE-2026-29081	Frappe is a full-stack web application framework. Prior to versions 14.100.1 and 15.100.0, an endpoint was vulnerable to SQL injection through specially crafted requests, which would allow a malicious actor to extract sensitive information. This issue has been patched in versions 14.100.1 and 15.100.0.	6.5	More Details
CVE-2026-28394	OpenClaw versions prior to 2026.2.15 contain a denial of service vulnerability in the web_fetch tool that allows attackers to crash the Gateway process through memory exhaustion by parsing oversized or deeply nested HTML responses. Remote attackers can social-engineer users into fetching malicious URLs with pathological HTML structures to exhaust server memory and cause service unavailability.	6.5	More Details
CVE-2026-28395	OpenClaw version 2026.1.14-1 prior to 2026.2.12 contain an improper network binding vulnerability in the Chrome extension (must be installed and enabled) relay server that treats wildcard hosts as loopback addresses, allowing the relay HTTP/WS server to bind to all interfaces when a wildcard cdpUrl is configured. Remote attackers can access relay HTTP endpoints off-host to leak service presence and	6.5	More Details

	port information, or conduct denial-of-service and brute-force attacks against the relay token header.		
CVE-2026-28467	OpenClaw versions prior to 2026.2.2 contain a server-side request forgery vulnerability in attachment and media URL hydration that allows remote attackers to fetch arbitrary HTTP(S) URLs. Attackers who can influence media URLs through model-controlled sendAttachment or auto-reply mechanisms can trigger SSRF to internal resources and exfiltrate fetched response bytes as outbound attachments.	6.5	More Details
CVE-2026-28480	OpenClaw versions prior to 2026.2.14 contain an authorization bypass vulnerability where Telegram allowlist matching accepts mutable usernames instead of immutable numeric sender IDs. Attackers can spoof identity by obtaining recycled usernames to bypass allowlist restrictions and interact with bots as unauthorized senders.	6.5	More Details
CVE-2026-28481	OpenClaw versions 2026.1.30 and earlier, contain an information disclosure vulnerability, patched in 2026.2.1, in the MS Teams attachment downloader (optional extension must be enabled) that leaks bearer tokens to allowlisted suffix domains. When retrying downloads after receiving 401 or 403 responses, the application sends Authorization bearer tokens to untrusted hosts matching the permissive suffix-based allowlist, enabling token theft.	6.5	More Details
CVE-2018-25162	2-Plan Team 1.0.4 contains an arbitrary file upload vulnerability that allows authenticated attackers to upload executable PHP files by sending multipart form data to managefile.php. Attackers can upload PHP files through the userfile1 parameter with action=upload, which are stored in the files directory and executed by the web server for remote code execution.	6.5	More Details
CVE-2026-29606	OpenClaw versions prior to 2026.2.14 contain a webhook signature-verification bypass in the voice-call extension that allows unauthenticated requests when the tunnel.allowNgrokFreeTierLoopbackBypass option is explicitly enabled. An external attacker can send forged requests to the publicly reachable webhook endpoint without a valid X-Twilio-Signature header, resulting in unauthorized webhook event handling and potential request flooding attacks.	6.5	More Details
CVE-2026-28685	Kimai is a web-based multi-user time-tracking application. Prior to version 2.51.0, "GET /api/invoices/{id}" only checks the role-based view_invoice permission but does not verify the requesting user has access to the invoice's customer. Any user with ROLE_TEAMLEAD (which grants view_invoice) can read all invoices in the system, including those belonging to customers assigned to other teams. This issue has been patched in version 2.51.0.	6.5	More Details
CVE-2026-22723	Inappropriate user token revocation due to a logic error in the token revocation endpoint implementation in Cloudfoundry UAA v77.30.0 to v78.7.0 and in Cloudfoundry Deployment v48.7.0 to v54.10.0.	6.5	More Details
CVE-2026-27770	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-25877	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.1, the application performs authorization checks based solely on the project_id parameter when handling chart-related operations (update, delete, etc.). No authorization check is performed against the chart_id itself. This allows an authenticated user who has access to any project to manipulate or access charts belonging to other users/ project. This issue has been patched in version 4.8.1.	6.5	More Details
CVE-2026-28682	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to version 2.2.3, the upload status SSE implementation on /uploadStatus publishes global upload state to any authenticated listener and includes file_id values that are not scoped to the requesting user. This issue has been patched in version 2.2.3.	6.4	More Details
CVE-2026-24316	SAP NetWeaver Application Server for ABAP provides an ABAP Report for testing purposes, which allows to send HTTP requests to arbitrary internal or external endpoints. The report is therefore vulnerable to Server-Side Request Forgery (SSRF). Successful exploitation could lead to interaction with potentially sensitive internal endpoints, resulting in a low impact on data confidentiality and integrity. There is no impact on availability of the application.	6.4	More Details
CVE-2026-2355	The My Calendar – Accessible Event Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `template` attribute of the `[my_calendar_upcoming]` shortcode in all versions up to, and including, 3.7.3. This is due to the use of `stripcslashes()` on user-supplied shortcode attribute values in the `mc_draw_template()` function, which decodes C-style hex escape sequences (e.g., `\x3c` to `<`) at render time, bypassing WordPress's `wp_kses_post()` content sanitization that runs at save time. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2026-1902	The Hammas Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'apix' parameter in the 'hp-calendar-manage-redirect' shortcode in all versions up to, and including, 1.5.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3228	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `[nxs_fbembed]` shortcode in all versions up to, and including, 4.4.6. This is due to insufficient input sanitization and output escaping on the `snapFB` post meta value. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1236	The Envira Gallery for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'justified_gallery_theme' parameter in all versions up to, and including, 1.12.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3034	The OoohBoi Steroids for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _ob_spacerat_link, _ob_bbad_link, and _ob_teleporter_link URL parameters in all versions up to, and including, 2.1.24. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user clicks on the injected element.	6.4	More Details
CVE-2026-1825	The Show YouTube video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'syv' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1824	The Infomaniak Connect for OpenID plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'endpoint_login' parameter of the infomaniak_connect_generic_auth_url shortcode in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1823	The Consensus Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's consensus shortcode in all versions up to, and including, 1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1820	The Media Library Alt Text Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bvmalt_sc_div_update_alt_text' shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1805	The DA Media GigList plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's damedia_giglist shortcode in all versions up to, and including, 1.9.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-28343	CKEditor 5 is a modern JavaScript rich-text editor with an MVC architecture. Prior to version 47.6.0, a cross-site scripting (XSS) vulnerability has been discovered in the General HTML Support feature. This vulnerability could be triggered by inserting specially crafted markup, leading to unauthorized JavaScript code execution, if the editor instance used an unsafe General HTML Support configuration. This issue has been patched in version 47.6.0.	6.4	More Details
CVE-2026-1574	The MyQtip – easy qTip2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `myqtip` shortcode in all versions up to, and including, 2.0.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-	The Wueen plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `wueen-blocket` shortcode in all versions up to, and including, 0.2.0 due to insufficient input sanitization and		More

2026-1569	output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	Details
CVE-2026-24309	Due to missing authorization check in SAP NetWeaver Application Server for ABAP, an authenticated attacker could execute specific ABAP function module to read, modify or insert entries into the database configuration table of the ABAP system. This unauthorized content change could lead to reduced system performance or interruptions. The vulnerability has low impact on the application's integrity and availability, with no effect on confidentiality.	6.4	More Details
CVE-2026-28036	Server-Side Request Forgery (SSRF) vulnerability in SkatDesign Ratatouille ratatouille allows Server Side Request Forgery.This issue affects Ratatouille: from n/a through <= 1.2.6.	6.4	More Details
CVE-2026-27684	SAP NetWeaver Feedback Notifications Service contains a SQL injection vulnerability that allows an authenticated attacker to inject arbitrary SQL code through user-controlled input fields. The application concatenates these inputs directly into SQL queries without proper validation or escaping. As a result, an attacker can manipulate the WHERE clause logic and potentially gain unauthorized access to or modify database information. This vulnerability has no impact on integrity and low impact on the confidentiality and availability of the application.	6.4	More Details
CVE-2026-28800	Natro Macro is an open-source Bee Swarm Simulator macro written in AutoHotkey. Prior to version 1.1.0, anyone with Discord Remote Control set up in a non-private channel gives access to any user with the permission to send message in said channel access to do anything on their computer. This includes keyboard and mouse inputs and full file access. This issue has been patched in version 1.1.0.	6.4	More Details
CVE-2026-2593	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `_gspb_post_css` post meta value and the `dynamicAttributes` block attribute in all versions up to, and including, 12.8.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3724	A weakness has been identified in SourceCodester Patients Waiting Area Queue Management System 1.0. This impacts an unknown function of the file /checkin.php. This manipulation of the argument patient_id causes improper authorization. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-3733	A vulnerability was detected in xuxueli xxl-job up to 3.3.2. This impacts an unknown function of the file source-code/src/main/java/com/xxl/job/admin/controller/JobInfoController.java. The manipulation results in server-side request forgery. It is possible to launch the attack remotely. The exploit is now public and may be used. The project maintainer closed the issue report with the following statement: "Access token security verification is required." (translated from Chinese)	6.3	More Details
CVE-2026-3791	A vulnerability has been found in SourceCodester Sales and Inventory System 1.0. Affected by this issue is some unknown functionality of the file dashboard.php of the component Search. The manipulation of the argument searchtxt leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-3725	A flaw has been found in 1024-lab/lab1024 SmartAdmin up to 3.29. Affected by this issue is the function freemarkerResolverContent of the file sa-base/src/main/java/net/lab1024/sa/base/module/support/mail/MailService.java of the component FreeMarker Template Handler. Executing a manipulation of the argument template_content can lead to improper neutralization of special elements used in a template engine. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3792	A vulnerability was found in SourceCodester Sales and Inventory System 1.0. This affects an unknown part of the file purchase_invoice.php of the component GET Parameter Handler. The manipulation of the argument purchaseid results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-3793	A vulnerability was determined in SourceCodester Sales and Inventory System 1.0. This vulnerability affects unknown code of the file sales_invoice1.php of the component GET Parameter Handler. This manipulation of the argument sellid causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-	A vulnerability was determined in Planet ICG-2510 1.0_20250811. The impacted element is the function sub_40C8E4 of the file /usr/sbin/httpd of the component Language Package Configuration Handler. Executing a manipulation of the argument Language can lead to stack-based buffer overflow.	6.3	More Details

3697	The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-3749	A weakness has been identified in Bytedesk up to 1.3.9. This vulnerability affects the function handleFileUpload of the file source-code/src/main/java/com/bytedesk/core/upload/UploadRestService.java of the component SVG File Handler. Executing a manipulation can lead to unrestricted upload. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 1.4.5.1 is able to resolve this issue. This patch is called 975e39e4dd527596987559f56c5f9f973f64eff7. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-3683	A vulnerability was detected in bufanyun HotGo up to 2.0. This issue affects the function ImageTransferStorage of the file /server/internal/logic/common/upload.go of the component Endpoint. The manipulation results in server-side request forgery. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3682	A security vulnerability has been detected in welovemedia FFmate up to 2.0.15. This vulnerability affects the function Execute of the file /internal/service/ffmpeg/ffmpeg.go. The manipulation leads to argument injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3681	A weakness has been identified in welovemedia FFmate up to 2.0.15. This affects the function fireWebhook of the file /internal/service/webhook/webhook.go. Executing a manipulation can lead to server-side request forgery. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3680	A security flaw has been discovered in RyuzakiShinji biome-mcp-server up to 1.0.0. Affected by this issue is some unknown functionality of the file biome-mcp-server.ts. Performing a manipulation results in command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The patch is named 335e1727147efeef011f1ff8b05dd751d8a660be. Applying a patch is the recommended action to fix this issue.	6.3	More Details
CVE-2026-3795	A security flaw has been discovered in doramart DoraCMS 3.0.x. Impacted is the function createFileBypath of the file /DoraCMS/server/app/router/api/v1.js. Performing a manipulation results in path traversal. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3790	A flaw has been found in SourceCodester Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file check_supplier_details.php of the component POST Parameter Handler. Executing a manipulation of the argument stock_name1 can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-3789	A vulnerability was detected in Bytedesk up to 1.3.9. Affected is the function getModels of the file source-code/src/main/java/com/bytedesk/ai/springai/providers/gitee/SpringAIGiteeRestService.java of the component SpringAIGiteeRestController. Performing a manipulation of the argument apiUrl results in server-side request forgery. Remote exploitation of the attack is possible. The exploit is now public and may be used. Upgrading to version 1.4.5.4 is able to address this issue. The patch is named 975e39e4dd527596987559f56c5f9f973f64eff7. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-3788	A security vulnerability has been detected in Bytedesk up to 1.3.9. This impacts the function getModels of the file source-code/src/main/java/com/bytedesk/ai/springai/providers/openrouter/SpringAIOpenrouterRestService.java of the component SpringAIOpenrouterRestController. Such manipulation of the argument apiUrl leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.4.5.4 will fix this issue. The name of the patch is 975e39e4dd527596987559f56c5f9f973f64eff7. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-3786	A security flaw has been discovered in EasyCMS up to 1.6. The impacted element is an unknown function of the file /RbacuserAction.class.php of the component Request Parameter Handler. The manipulation of the argument _order results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. This		

2026-3737	affects an unknown part of the file add_user.php of the component User Creation Handler. Executing a manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-3785	A vulnerability was identified in EasyCMS up to 1.6. The affected element is an unknown function of the file /RbacnodeAction.class.php of the component Request Parameter Handler. The manipulation of the argument _order leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3771	A vulnerability has been found in SourceCodester/janobe Resort Reservation System 1.0. This vulnerability affects unknown code of the file /accomodation.php. Such manipulation of the argument q leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-28071	Missing Authorization vulnerability in PixFort pixfort Core pixfort-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects pixfort Core: from n/a through <= 3.2.22.	6.3	More Details
CVE-2026-3738	A vulnerability was identified in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the component Financial Report Page. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-3767	A weakness has been identified in itsourcecode sanitize or validate this input 1.0. Affected is an unknown function of the file /admin/teacher-attendance.php. Executing a manipulation of the argument teacher_id can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-3756	A vulnerability was identified in SourceCodester Sales and Inventory System up to 1.0. Affected is an unknown function of the file /check_item_details.php. The manipulation of the argument stock_name1 leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-3797	A security vulnerability has been detected in Tiandy Video Surveillance System 视频监控平台 7.17.0. The impacted element is the function uploadFile of the file /src/com/tiandy/easy7/core/rest/CLS_REST_File.java. The manipulation of the argument fileName leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3754	A vulnerability was found in SourceCodester Sales and Inventory System 1.0. This affects an unknown function of the file /add_stock.php. Performing a manipulation of the argument cost results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-3739	A security flaw has been discovered in suitenumerique messages 0.2.0. This issue affects the function ThreadAccessSerializer of the file src/backend/core/api/serializers.py of the component ThreadAccess. The manipulation results in improper authentication. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.3.0 is capable of addressing this issue. The patch is identified as d7729f4b885449f6dee3faf8b5f2a05769fb3d6e. The affected component should be upgraded.	6.3	More Details
CVE-2026-3753	A vulnerability has been found in SourceCodester Sales and Inventory System up to 1.0. The impacted element is an unknown function of the file /add_sales_print.php. Such manipulation of the argument sid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-3745	A vulnerability was found in code-projects Student Web Portal 1.0. Affected is an unknown function of the file profile.php. The manipulation of the argument User results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-3748	A security flaw has been discovered in Bytedesk up to 1.3.9. This affects the function uploadFile of the file source-code/src/main/java/com/bytedesk/core/upload/UploadRestController.java of the component SVG File Handler. Performing a manipulation results in unrestricted upload. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.4.5.1 is able to mitigate this issue. The patch is named 975e39e4dd527596987559f56c5f9f973f64eff7. Upgrading the affected component is recommended.	6.3	More Details
	A vulnerability was determined in SourceCodester Sales and Inventory System 1.0. This impacts an		

CVE-2026-3755	unknown function of the file /check_customer_details.php of the component POST Handler. Executing a manipulation of the argument stock_name1 can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-3672	A vulnerability has been found in JeecgBoot up to 3.9.1. Affected is the function isExistSqlInjectKeyword of the file /jeecg-boot/sys/api/getDictItems. Such manipulation leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-3800	A vulnerability has been found in SourceCodester/janobe Resort Reservation System 1.0. Affected is the function doInsert of the file /controller.php?action=add. Such manipulation of the argument image leads to unrestricted upload. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-26982	Ghostty is a cross-platform terminal emulator. Ghostty allows control characters such as 0x03 (Ctrl+C) in pasted and dropped text. These can be used to execute arbitrary commands in some shell environments. This attack requires an attacker to convince the user to copy and paste or drag and drop malicious text. The attack requires user interaction to be triggered, but the dangerous characters are invisible in most GUI environments so it isn't trivially detected, especially if the string contents are complex. Fixed in Ghostty v1.3.0.	6.3	More Details
CVE-2026-3806	A weakness has been identified in SourceCodester/janobe Resort Reservation System 1.0. This issue affects some unknown processing of the file /room_rates.php. This manipulation of the argument q causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-27605	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.4, the application allows uploading files (project logos) without validating the file type or content. It trusts the extension provided by the user. These files are saved to the uploads/ directory and served statically. An attacker can upload an HTML file containing malicious JavaScript. Since authentication tokens are likely stored in localStorage (as they are returned in the API body), this XSS can lead to account takeover. This issue has been patched in version 4.8.4.	6.3	More Details
CVE-2026-3813	A vulnerability was identified in opencc JFlow up to 5badc00db382d7cb82dad231e6a866b18e0addfe. Affected by this vulnerability is the function Calculate of the file src/main/java/bp/wf/httphandler/WF_CCForm.java. Such manipulation leads to injection. The attack may be performed from remote. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-3616	A vulnerability was detected in DefaultFuction Jeson Customer Relationship Management System 1.0.0. Impacted is an unknown function of the file /modules/customers/edit.php. Performing a manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. The patch is named f0e991870e9d33701cca3a1d0fd4eec135af01a6. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-28689	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, domain="path" authorization is checked before final file open/use. A symlink swap between check-time and use-time bypasses policy-denied read/write. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	6.3	More Details
CVE-2026-28509	LangBot is a global IM bot platform designed for LLMs. Prior to version 4.8.7, LangBot’s web UI renders user-supplied raw HTML using rehypeRaw, which can lead to a cross-site scripting (XSS) vulnerability. This issue has been patched in version 4.8.7.	6.3	More Details
CVE-2018-25184	Surreal ToDo 0.6.1.2 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the content parameter. Attackers can supply directory traversal sequences through the content parameter in index.php to access sensitive system files like configuration and initialization files.	6.2	More Details
CVE-2025-69648	GNU Binutils thru 2.45.1 readelf contains a denial-of-service vulnerability when processing a crafted binary with malformed DWARF .debug_rnglists data. A logic flaw in the DWARF parsing path causes readelf to repeatedly print the same warning message without making forward progress, resulting in a non-terminating output loop that requires manual interruption. No evidence of memory corruption or code execution was observed.	6.2	More Details
	GNU Binutils thru 2.45.1 readelf contains a denial-of-service vulnerability when processing a crafted		

CVE-2025-69647	binary with malformed DWARF loclists data. A logic flaw in the DWARF parsing code can cause readelf to repeatedly print the same table output without making forward progress, resulting in an unbounded output loop that never terminates unless externally interrupted. A local attacker can trigger this behavior by supplying a malicious input file, causing excessive CPU and I/O usage and preventing readelf from completing its analysis.	6.2	More Details
CVE-2026-28544	Race condition vulnerability in the printing module. Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2026-28539	Data processing vulnerability in the certificate management module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-41762	An unauthenticated attacker can abuse the weak hash of the backup generated by the wwwdnload.cgi endpoint to gain unauthorized access to sensitive data, including password hashes and certificates.	6.2	More Details
CVE-2025-69652	GNU Binutils thru 2.46 readelf contains a vulnerability that leads to an abort (SIGABRT) when processing a crafted ELF binary with malformed DWARF abbrev or debug information. Due to incomplete state cleanup in process_debug_info(), an invalid debug_info_p state may propagate into DWARF attribute parsing routines. When certain malformed attributes result in an unexpected data length of zero, byte_get_little_endian() triggers a fatal abort. No evidence of memory corruption or code execution was observed; the impact is limited to denial of service.	6.2	More Details
CVE-2018-25198	eToolz 3.4.8.0 contains a denial of service vulnerability that allows local attackers to crash the application by supplying oversized input buffers. Attackers can create a payload file containing 255 bytes of data that triggers a buffer overflow condition when processed by the application.	6.2	More Details
CVE-2026-25169	Divide by zero in Microsoft Graphics Component allows an unauthorized attacker to deny service locally.	6.2	More Details
CVE-2026-25168	Null pointer dereference in Microsoft Graphics Component allows an unauthorized attacker to deny service locally.	6.2	More Details
CVE-2026-29048	HumHub is an Open Source Enterprise Social Network. In version 1.18.0, a cross-site scripting vulnerability was identified in the Button component of version 1.18.0. Due to inconsistent output encoding at several points within the software, malicious scripts could be injected and executed in the context of the user's browser. This issue has been patched in version 1.18.1.	6.1	More Details
CVE-2026-28772	A Reflected Cross-Site Scripting (XSS) vulnerability in the /IDC_Logging/index.cgi endpoint of International Datacasting Corporation (IDC) SFX Series SuperFlex SatelliteReceiver Web Management Interface version 101 allows a remote attacker to execute arbitrary web scripts or HTML. The vulnerability is triggered by sending a crafted payload through the `submitType` parameter, which is reflected directly into the DOM without proper escaping.	6.1	More Details
CVE-2026-26195	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, stored xss is still possible through unsafe template rendering that mixes user input with safe plus permissive sanitizer handling of data urls. This issue has been patched in version 0.14.2.	6.1	More Details
CVE-2026-20023	A vulnerability in the OSPF protocol of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to corrupt memory on an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to memory corruption when parsing OSPF protocol packets. An attacker could exploit this vulnerability by sending crafted OSPF packets to an affected device. A successful exploit could allow the attacker to cause memory corruption causing the affected device to reboot, resulting in a DoS condition.	6.1	More Details
CVE-2026-28222	Wagtail is an open source content management system built on Django. Prior to versions 6.3.8, 7.0.6, 7.2.3, and 7.3.1, a stored cross-site scripting (XSS) vulnerability exists on rendering TableBlock blocks within a StreamField. A user with access to create or edit pages containing TableBlock StreamField blocks is able to set specially-crafted class attributes on the block which run arbitrary JavaScript code when the page is viewed. When viewed by a user with higher privileges, this could lead to performing actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin, and only affects sites using TableBlock. This issue has been patched in versions 6.3.8, 7.0.6, 7.2.3, and 7.3.1.	6.1	More Details

CVE-2026-29052	The Calendar module for HumHub enables users to create one-time or recurring events, manage attendee invitations, and efficiently track all scheduled activities. Prior to version 1.8.11, a Stored Cross-Site Scripting (XSS) vulnerability in the Event Types of the HumHub Calendar module impacts users viewing events created by an administrative account. This issue has been patched in version 1.8.11.	6.1	More Details
CVE-2026-20022	A vulnerability in the OSPF protocol of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition when OSPF canonicalization debug is enabled by using the command debug ip ospf canon. This vulnerability is due to insufficient input validation when processing OSPF LSU packets. An attacker could exploit this vulnerability by sending crafted unauthenticated OSPF packets. A successful exploit could allow the attacker to write to memory outside of the packet data, causing the device to reload, resulting in a DoS condition.	6.1	More Details
CVE-2026-29038	changedetection.io is a free open source web page change detection tool. Prior to version 0.54.4, there is a reflected cross-site scripting (XSS) vulnerability identified in the /rss/tag/ endpoint of changedetection.io. The tag_uuid path parameter is reflected directly in the HTTP response body without HTML escaping. Since Flask returns text/html by default for plain string responses, the browser parses and executes injected JavaScript. This issue has been patched in version 0.54.4.	6.1	More Details
CVE-2026-20149	A vulnerability in Cisco Webex could have allowed an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. Cisco has addressed this vulnerability, and no customer action is needed. This vulnerability was due to improper filtering of user-supplied input. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to conduct an XSS attack against the targeted user.	6.1	More Details
CVE-2026-20102	A vulnerability in the SAML 2.0 single sign-on (SSO) feature of Cisco Secure Firewall ASA Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the SAML feature and access sensitive, browser-based information. This vulnerability is due to insufficient input validation of multiple HTTP parameters. An attacker could exploit this vulnerability by persuading a user to access a malicious link. A successful exploit could allow the attacker&nbsp;to conduct a reflected XSS attack through an affected device.	6.1	More Details
CVE-2026-20070	A vulnerability in the VPN web services component of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a browser that is accessing an affected device.&nbsp; This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by persuading a user to follow a link to a malicious website that is designed to submit malicious input to the affected application. A successful exploit could allow the attacker to execute arbitrary HTML or script code in the browser in the context of the VPN web server.	6.1	More Details
CVE-2026-28771	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the /index.cgi endpoint of International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver Web Management Interface version 101. The application fails to adequately sanitize user-supplied input provided via the `cat` parameter before reflecting it in the HTTP response, allowing a remote attacker to execute arbitrary HTML or JavaScript in the victim's browser context.	6.1	More Details
CVE-2026-22614	The encryption mechanism used in Eaton's EasySoft project file was insecure and susceptible to brute force attacks, an attacker with access to this file and the local host machine could potentially read the sensitive information stored and tamper with the project file. This security issue has been fixed in the latest version of Eaton EasySoft which is available on the Eaton download centre.	6.1	More Details
CVE-2026-31797	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap out-of-bounds read in CTiffImg::ReadLine() when iccApplyProfiles processes a crafted TIFF image, causing memory disclosure or crash. This vulnerability is fixed in 2.3.1.5.	6.1	More Details
CVE-2025-70025	An issue pertaining to CWE-79: Improper Neutralization of Input During Web Page Generation was discovered in benkeen generatedata 4.0.14.	6.1	More Details
CVE-2026-28486	OpenClaw versions 2026.1.16-2 prior to 2026.2.14 contain a path traversal vulnerability in archive extraction during installation commands that allows arbitrary file writes outside the intended directory. Attackers can craft malicious archives that, when extracted via skills install, hooks install, plugins install, or signal install commands, write files to arbitrary locations enabling persistence or code execution.	6.1	More Details
	The WP All Import – Drag & Drop Import for CSV, XML, Excel & Google Sheets plugin for WordPress is		

CVE-2026-2830	vulnerable to Reflected Cross-Site Scripting via the ‘filepath’ parameter in all versions up to, and including, 4.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-0489	Due to insufficient validation of user-controlled input in the URLs query parameter. SAP Business One Job Service could allow an unauthenticated attacker to inject specially crafted input which upon user interaction could result in a DOM-based Cross-Site Scripting (XSS) vulnerability. This issue had a low impact on the confidentiality and integrity of the application with no impact on availability.	6.1	More Details
CVE-2026-1706	The All-in-One Video Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'vi' parameter in all versions up to, and including, 4.7.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-30981	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-buffer-overflow read in CIccXmlArrayType<>::DumpArray() causing out-of-bounds read and/or crash. This vulnerability is fixed in 2.3.1.5.	6.1	More Details
CVE-2025-40638	A reflected Cross-Site Scripting (XSS) vulnerability has been found in Eventobot. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending him/her a malicious URL using the 'name' parameter in '/search-results'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	6.1	More Details
CVE-2026-28457	OpenClaw versions prior to 2026.2.14 contain a path traversal vulnerability in sandbox skill mirroring (must be enabled) that uses the skill frontmatter name parameter unsanitized when copying skills into the sandbox workspace. Attackers who provide a crafted skill package with traversal sequences like ../ or absolute paths in the name field can write files outside the sandbox workspace root directory.	6.1	More Details
CVE-2019-25502	Simple Job Script contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the job_type_value parameter in the jobs endpoint. Attackers can craft requests with SVG payload injection to execute arbitrary JavaScript in victim browsers and steal session cookies or perform unauthorized actions.	6.1	More Details
CVE-2026-30984	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap out-of-bounds read in CIccCalculatorFunc::ApplySequence() causing an application crash. This vulnerability is fixed in 2.3.1.5.	6.1	More Details
CVE-2026-30982	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap out-of-bounds read in CIccPcsXform::pushXYZConvert() causing crash and potentially leaking memory contents. This vulnerability is fixed in 2.3.1.5.	6.1	More Details
CVE-2026-28350	lxml_html_clean is a project for HTML cleaning functionalities copied from `lxml.html.clean`. Prior to version 0.4.4, the <base> tag passes through the default Cleaner configuration. While page_structure=True removes html, head, and title tags, there is no specific handling for <base>, allowing an attacker to inject it and hijack relative links on the page. This issue has been patched in version 0.4.4.	6.1	More Details
CVE-2026-28348	lxml_html_clean is a project for HTML cleaning functionalities copied from `lxml.html.clean`. Prior to version 0.4.4, the _has_sneaky_javascript() method strips backslashes before checking for dangerous CSS keywords. This causes CSS Unicode escape sequences to bypass the @import and expression() filters, allowing external CSS loading or XSS in older browsers. This issue has been patched in version 0.4.4.	6.1	More Details
CVE-2026-28223	Wagtail is an open source content management system built on Django. Prior to versions 6.3.8, 7.0.6, 7.2.3, and 7.3.1, a stored cross-site scripting (XSS) vulnerability exists on confirmation messages within the wagtail.contrib.simple_translation module. A user with access to the Wagtail admin area may create a page with a specially-crafted title which, when another user performs the "Translate" action, causes arbitrary JavaScript code to run. This could lead to performing actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been patched in versions 6.3.8, 7.0.6, 7.2.3, and 7.3.1.	6.1	More Details
CVE-2026-27982	An open redirect vulnerability exists in django-allauth versions prior to 65.14.1 when SAML IdP initiated SSO is enabled (it is disabled by default), which may allow an attacker to redirect users to an arbitrary external website via a crafted URL.	6.1	More Details
CVE-2025-36173	Affected Product(s)Version(s)InfoSphere Data Architect9.2.1	6.1	More Details

CVE-2026-2431	The CM Custom Reports plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'date_from' and 'date_to' parameters in all versions up to, and including, 1.2.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-2433	The RSS Aggregator – RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via postMessage in all versions up to, and including, 5.0.11. This is due to the plugin's admin-shell.js registering a global message event listener without origin validation (missing event.origin check) and directly passing user-controlled URLs to window.open() without URL scheme validation. This makes it possible for unauthenticated attackers to execute arbitrary JavaScript in the context of an authenticated administrator's session by tricking them into visiting a malicious website that sends crafted postMessage payloads to the plugin's admin page.	6.1	More Details
CVE-2026-20044	A vulnerability in the lockdown mechanism of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, local attacker to perform arbitrary commands as root. This vulnerability is due to insufficient restrictions on remediation modules while in lockdown mode. An attacker could exploit this vulnerability by sending crafted input to the system CLI of the affected device. A successful exploit could allow the attacker to run arbitrary commands or code as root, even when the system is in lockdown mode. To exploit this vulnerability, the attacker must have valid administrative credentials.	6.0	More Details
CVE-2026-20008	A vulnerability in a small subset of CLI commands that are used on Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to craft Lua code that could be used on the underlying operating system as&nbsp;root. This vulnerability exists because user-provided input is not properly sanitized. An attacker could exploit this vulnerability by crafting valid Lua code and submitting it as a malicious parameter for a CLI command. A successful exploit could allow the attacker to inject Lua code, which could lead to arbitrary code execution as the root user. To exploit this vulnerability, an attacker must have valid&nbsp;Administrator&nbsp;credentials.	6.0	More Details
CVE-2026-20016	A vulnerability in the Cisco FXOS Software CLI feature for Cisco Secure Firewall ASA Software and Secure FTD Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit this vulnerability, the attacker must have valid administrative credentials on an affected device. This vulnerability is due to insufficient input validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input for specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	6.0	More Details
CVE-2025-49784	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer 6.4 all versions, FortiAnalyzer-BigData 7.6.0, FortiAnalyzer-BigData 7.4.0 through 7.4.4, FortiAnalyzer-BigData 7.2 all versions, FortiAnalyzer-BigData 7.0 all versions, FortiAnalyzer-BigData 6.4 all versions, FortiAnalyzer-BigData 6.2 all versions may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	6.0	More Details
CVE-2026-20017	A vulnerability in the CLI of Cisco Secure FTD Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as root. To exploit this vulnerability, the attacker must have valid administrative credentials on an affected device. This vulnerability is due to insufficient input validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input for a specific CLI command. A successful exploit could allow the attacker to execute commands on the underlying operating system as&nbsp;root.	6.0	More Details
CVE-2026-20063	A vulnerability in the CLI of Cisco Secure FTD Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as root. To exploit this vulnerability, the attacker must have valid administrative credentials on an affected device. This vulnerability is due to insufficient input validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input for a specific CLI command. A successful exploit could allow the attacker to execute commands on the underlying operating system as root.	6.0	More Details
CVE-2026-27138	Certificate verification can panic when a certificate in the chain has an empty DNS name and another certificate in the chain has excluded name constraints. This can crash programs that are either directly verifying X.509 certificate chains, or those that use TLS.	5.9	More Details
CVE-2026-	OpenClaw's voice-call plugin versions before 2026.2.3 contain an improper authentication vulnerability in webhook verification that allows remote attackers to bypass verification by supplying untrusted forwarded headers. Attackers can spoof webhook events by manipulating Forwarded or X-Forwarded-*	5.9	More Details

28465	headers in reverse-proxy configurations that implicitly trust these headers.		
CVE-2026-30247	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.12, the application's "Import document via URL" feature is vulnerable to Server-Side Request Forgery (SSRF) through HTTP redirects. While the backend implements comprehensive URL validation (blocking private IPs, loopback addresses, reserved hostnames, and cloud metadata endpoints), it fails to validate redirect targets. An attacker can bypass all protections by using a redirect chain, forcing the server to access internal services. Additionally, Docker-specific internal addresses like host.docker.internal are not blocked. This issue has been patched in version 0.2.12.	5.9	More Details
CVE-2026-20018	A vulnerability in the sftunnel functionality of Cisco Secure Firewall Management Center (FMC) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker with administrative privileges to write arbitrary files as root on the underlying operating system. This vulnerability is due to insufficient validation of the directory path during file synchronization. An attacker could exploit this vulnerability by crafting a directory path outside of the expected file location. A successful exploit could allow the attacker to create or replace any file on the underlying operating system.	5.9	More Details
CVE-2026-26310	Envoy is a high-performance edge/middle/service proxy. Prior to 1.37.1, 1.36.5, 1.35.8, and 1.34.13, calling Utility::getAddressWithPort with a scoped IPv6 addresses causes a crash. This utility is called in the data plane from the original_src filter and the dns filter. This vulnerability is fixed in 1.37.1, 1.36.5, 1.35.8, and 1.34.13.	5.9	More Details
CVE-2026-27801	Vaultwarden is an unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. Vaultwarden versions 1.34.3 and prior are susceptible to a 2FA bypass when performing protected actions. An attacker who gains authenticated access to a user’s account can exploit this bypass to perform protected actions such as accessing the user’s API key or deleting the user’s vault and organisations the user is an admin/owner of . This issue has been patched in version 1.35.0.	5.9	More Details
CVE-2026-3638	Improper access control in user and role restore API endpoints in Devolutions Server 2025.3.11.0 and earlier allows a low-privileged authenticated user to restore deleted users and roles via crafted API requests.	5.9	More Details
CVE-2026-29076	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to version 0.37.0, cpp-httplib uses std::regex (libstdc++) to parse RFC 5987 encoded filename* values in multipart Content-Disposition headers. The regex engine in libstdc++ implements backtracking via deep recursion, consuming one stack frame per input character. An attacker can send a single HTTP POST request with a crafted filename* parameter that causes uncontrolled stack growth, resulting in a stack overflow (SIGSEGV) that crashes the server process. This issue has been patched in version 0.37.0.	5.9	More Details
CVE-2026-30856	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.3.0, a vulnerability involving tool name collision and indirect prompt injection allows a malicious remote MCP server to hijack tool execution. By exploiting an ambiguous naming convention in the MCP client (mcp_{service}_{tool}), an attacker can register a malicious tool that overwrites a legitimate one (e.g., tavily_extract). This enables the attacker to redirect LLM execution flow, exfiltrate system prompts, context, and potentially execute other tools with the user's privileges. This issue has been patched in version 0.3.0.	5.9	More Details
CVE-2026-26311	Envoy is a high-performance edge/middle/service proxy. Prior to 1.37.1, 1.36.5, 1.35.8, and 1.34.13, a logic vulnerability in Envoy's HTTP connection manager (FilterManager) that allows for Zombie Stream Filter Execution. This issue creates a "Use-After-Free" (UAF) or state-corruption window where filter callbacks are invoked on an HTTP stream that has already been logically reset and cleaned up. The vulnerability resides in source/common/http/filter_manager.cc within the FilterManager::decodeData method. The ActiveStream object remains valid in memory during the deferred deletion window. If a DATA frame arrives on this stream immediately after the reset (e.g., in the same packet processing cycle), the HTTP/2 codec invokes ActiveStream::decodeData, which cascades to FilterManager::decodeData. FilterManager::decodeData fails to check the saw_downstream_reset_ flag. It iterates over the decoder_filters_ list and invokes decodeData() on filters that have already received onDestroy(). This vulnerability is fixed in 1.37.1, 1.36.5, 1.35.8, and 1.34.13.	5.9	More Details
CVE-2026-23656	Insufficient verification of data authenticity in Windows App Installer allows an unauthorized attacker to perform spoofing over a network.	5.9	More Details
CVE-2026-	Path traversal vulnerability in the certificate management module. Impact: Successful exploitation of	5.9	More

28538	this vulnerability may affect availability.		Details
CVE-2026-29613	OpenClaw versions prior to 2026.2.12 contain a vulnerability in the BlueBubbles (optional plugin) webhook handler in which it authenticates requests based solely on loopback remoteAddress without validating forwarding headers, allowing bypass of configured webhook passwords. When the gateway operates behind a reverse proxy, unauthenticated remote attackers can inject arbitrary BlueBubbles message and reaction events by reaching the proxy endpoint.	5.9	More Details
CVE-2026-28546	Buffer overflow vulnerability in the scanning module. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2025-13219	IBM Aspera Orchestrator 3.0.0 through 4.1.2 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history.	5.9	More Details
CVE-2026-28545	Race condition vulnerability in the printing module. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2024-35644	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pascal Birchler Preferred Languages allows DOM-Based XSS.This issue affects Preferred Languages: from n/a through 2.2.2.	5.9	More Details
CVE-2026-28464	OpenClaw versions prior to 2026.2.12 use non-constant-time string comparison for hook token validation, allowing attackers to infer tokens through timing measurements. Remote attackers with network access to the hooks endpoint can exploit timing side-channels across multiple requests to gradually determine the authentication token.	5.9	More Details
CVE-2026-27686	Due to a Missing Authorization Check in SAP Business Warehouse (Service API), an authenticated attacker could perform unauthorized actions via an affected RFC function module. Successful exploitation could enable unauthorized configuration and control changes, potentially disrupting request processing and causing denial of service. This results in low impact on integrity and high impact on availability, while confidentiality remains unaffected.	5.9	More Details
CVE-2026-30850	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.9 and 9.5.0-alpha.9, the file metadata endpoint (GET /files/:appId/metadata/:filename) does not enforce beforeFind / afterFind file triggers. When these triggers are used as access-control gates, the metadata endpoint bypasses them entirely, allowing unauthorized access to file metadata. This issue has been patched in versions 8.6.9 and 9.5.0-alpha.9.	5.9	More Details
CVE-2025-2399	Improper Validation of Specified Index, Position, or Offset in Input vulnerability in Mitsubishi Electric CNC M800V Series M800VW and M800VS, M80V Series M80V and M80VW, M800 Series M800W and M800S, M80 Series M80 and M80W, E80 Series E80, C80 Series C80, M700V Series M750VW, M720VW, 730VW, M720VS, M730VS, and M750VS, M70V Series M70V, E70 Series E70, and Software Tools NC Trainer2 and NC Trainer2 plus allows a remote attacker to cause an out-of-bounds read, resulting in a denial-of-service condition by sending specially crafted packets to TCP port 683.	5.9	More Details
CVE-2026-20057	Multiple Cisco products are affected by a vulnerability in the Snort 3 Visual Basic for Applications (VBA) feature which could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to crash.&nbsp; &nbsp; This vulnerability is due to lack of proper error checking when decompressing VBA data. An attacker could exploit this vulnerability by sending a crafted VBA data to the Snort 3 Detection Engine on the targeted device. A successful exploit could allow the attacker to cause the Snort 3 Detection Engine to unexpectedly restart causing a a denial of service (DoS) condition.	5.8	More Details
CVE-2026-20065	Multiple Cisco products are affected by a vulnerability in the Snort 3 Detection Engine that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart, resulting in an interruption of packet inspection. This vulnerability is due to an error in the binder module initialization logic of the Snort Detection Engine. An attacker could exploit this vulnerability by sending certain packets through an established connection that is parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine restarts unexpectedly.	5.8	More Details
CVE-2026-20058	Multiple Cisco products are affected by vulnerabilities in the Snort 3 VBA feature that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to crash. These vulnerabilities are due to improper error checking when decompressing VBA data. An attacker could exploit these vulnerabilities by sending crafted VBA data to the Snort 3 Detection Engine on the targeted device. A successful exploit could allow the attacker to cause the Snort 3 Detection Engine to unexpectedly restart, causing a DoS condition.	5.8	More Details

CVE-2026-20068	Multiple Cisco products are affected by a vulnerability in the Snort 3 detection engine that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart, resulting in an interruption of packet inspection. This vulnerability is due to incomplete error checking when parsing remote procedure call (RPC) data. An attacker could exploit this vulnerability by sending crafted RPC packets through an established connection to be parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine unexpectedly restarts.	5.8	More Details
CVE-2026-20066	Multiple Cisco products are affected by a vulnerability in the Snort 3 Detection Engine that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart, resulting in an interruption of packet inspection. This vulnerability is due to an error in the JSTokenizer normalization logic when the HTTP inspection normalizes JavaScript. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection that is parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine restarts unexpectedly. JSTokenizer is not enabled by default.	5.8	More Details
CVE-2026-20067	Multiple Cisco products are affected by a vulnerability in the Snort 3 detection engine that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart, resulting in an interruption of packet inspection.&nbsp; This vulnerability is due to incomplete error checking when parsing the Multicast DNS fields of the HTTP header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection to be parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine unexpectedly restarts.	5.8	More Details
CVE-2026-20053	Multiple Cisco products are affected by a vulnerability in the Snort 3 VBA feature that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to crash. This vulnerability is due to improper range checking when decompressing VBA data, which is user controlled. An attacker could exploit this vulnerability by sending crafted VBA data to the Snort 3 Detection Engine on the targeted device. A successful exploit could allow the attacker to cause an overflow of heap data, which could cause a DoS condition.	5.8	More Details
CVE-2026-20073	A vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to send traffic that should be denied through an affected device. This vulnerability is due to improper error handling when an affected device that is joining a cluster runs out of memory while replicating access control rules. An attacker could exploit this vulnerability by sending traffic that should be blocked through the device. A successful exploit could allow the attacker to bypass access controls and reach devices in protected networks.	5.8	More Details
CVE-2026-20005	Multiple Cisco products are affected by a vulnerability in the Snort 3 Detection Engine that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart, resulting in an interruption of packet inspection. This vulnerability is due to incomplete parsing of the SSL handshake ingress packets. An attacker could exploit this vulnerability by sending crafted SSL handshake packets. A successful exploit could allow the attacker to cause a denial of service (DoS) condition when the Snort 3 Detection Engine restarts unexpectedly.	5.8	More Details
CVE-2025-54659	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] vulnerability in Fortinet FortiSOAR Agent Communication Bridge 1.1.0, FortiSOAR Agent Communication Bridge 1.0 all versions may allow an unauthenticated attacker to read files accessible to the fortisoar user on a system where the agent is deployed, via sending a crafted request to the agent port.	5.8	More Details
CVE-2026-20054	Multiple Cisco products are affected by a vulnerability in the Snort 3 VBA feature that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to crash.&nbsp; This vulnerability is due to improper error checking when decompressing VBA data. An attacker could exploit this vulnerability by sending crafted VBA data to the Snort 3 Detection Engine on the targeted device. A successful exploit could allow the attacker to cause the Snort 3 Detection Engine to enter an infinite loop, causing a DoS condition.	5.8	More Details
CVE-2025-68515	Insertion of Sensitive Information Into Sent Data vulnerability in Roland Murg WP Booking System wp-booking-system allows Retrieve Embedded Sensitive Data.This issue affects WP Booking System: from n/a through <= 2.0.19.12.	5.8	More Details
CVE-2026-20052	A vulnerability in the memory management handling for the Snort 3 Detection Engine of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart. This vulnerability is due to a logic error in memory management when a device is performing Snort 3 SSL packet inspection. An attacker could exploit this vulnerability by sending crafted SSL packets&nbsp;through an established connection to be parsed by the Snort 3 Detection Engine. A successful exploit could allow the attacker to cause a denial of service (DoS) condition when the Snort 3 Detection Engine unexpectedly restarts.	5.8	More Details

CVE-2026-20015	A vulnerability in the IKEv2 feature of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device that may impact the availability of services to devices elsewhere in the network. This vulnerability is due to a memory leak when parsing IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to exhaust resources, causing a DoS condition that will eventually require the device to be manually reloaded.	5.8	More Details
CVE-2026-20006	A vulnerability in the TLS cryptography functionality of the Snort 3 Detection Engine of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to unexpectedly restart, resulting in a denial of service (DoS) condition. This vulnerability is due to improper implementation of the TLS protocol. An attacker could exploit this vulnerability by sending a crafted TLS packet to an affected system. A successful exploit could allow the attacker to cause a device that is running Cisco Secure FTD Software to drop network traffic, resulting in a DoS condition.&nbsp; Note: TLS 1.3 is not affected by this vulnerability.	5.8	More Details
CVE-2026-20007	A vulnerability in the Snort 2 and Snort 3 deep packet inspection of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured Snort rules and allow traffic onto the network that should have been dropped. This vulnerability is due to a logic error in the integration of the Snort Engine rules with Cisco Secure FTD Software that could allow different Snort rules to be hit when deep inspection of the packet is performed for the inner and outer connections. An attacker could exploit this vulnerability by sending crafted traffic to a targeted device that would hit configured Snort rules. A successful exploit could allow the attacker to send traffic to a network where it should have been denied.	5.8	More Details
CVE-2026-27687	Due to missing authorization check in SAP S/4HANA HCM Portugal and SAP ERP HCM Portugal, a user with high privileges could access sensitive data belonging to another company. This vulnerability has a high impact on confidentiality and does not affect integrity and availability.	5.8	More Details
CVE-2026-20013	A vulnerability in the IKEv2 feature of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device that may also impact the availability of services to devices elsewhere in the network. This vulnerability is due to memory exhaustion caused by not freeing memory during IKEv2 packet processing. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to exhaust resources, causing a DoS condition that will eventually require the device to manually reload.	5.8	More Details
CVE-2024-43035	Fonoster 0.5.5 before 0.6.1 allows ../ directory traversal to read arbitrary files via the /sounds/:file or /tts/:file VoiceServer endpoint. This occurs in serveFiles in mods/voice/src/utils.ts. NOTE: serveFiles exists in 0.5.5 but not in the next release, 0.6.1.	5.8	More Details
CVE-2026-30883	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, an extremely large image profile could result in a heap overflow when encoding a PNG image. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	5.7	More Details
CVE-2026-24311	The SAP Customer Checkout application exhibits certain design characteristics that involve locally storing operational data using reversible protection mechanisms. Access to this data, combined with user?initiated interaction, may allow modifications to occur without validation. Such changes could affect system behaviour during startup, resulting in a high impact on the application's confidentiality and integrity, with a low impact on availability.	5.6	More Details
CVE-2026-27215	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to its availability. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-29612	OpenClaw versions prior to 2026.2.14 decode base64-backed media inputs into buffers before enforcing decoded-size budget limits, allowing attackers to trigger large memory allocations. Remote attackers can supply oversized base64 payloads to cause memory pressure and denial of service.	5.5	More Details
CVE-2026-27217	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to its availability. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27221	Acrobat Reader versions 24.001.30307, 24.001.30308, 25.001.21265 and earlier are affected by an Improper Certificate Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to spoof the identity of a signer. Exploitation of this issue requires user interaction.	5.5	More Details

CVE-2026-21363	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27218	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27281	DNG SDK versions 1.7.1 2471 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to cause the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-30936	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a crafted image could cause an out of bounds heap write inside the WaveletDenoiseImage method. When processing a crafted image with the -wavelet-denoise operation an out of bounds write can occur. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	5.5	More Details
CVE-2026-27214	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-26123	Cwe is not in rca categories in Microsoft Authenticator allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21364	Substance3D - Painter versions 11.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21365	Substance3D - Painter versions 11.1.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27216	Substance3D - Painter versions 11.1.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-69645	Binutils objdump contains a denial-of-service vulnerability when processing a crafted binary with malformed DWARF debug information. A logic error in the handling of DWARF compilation units can result in an invalid offset_size value being used inside byte_get_little_endian, leading to an abort (SIGABRT). The issue was observed in binutils 2.44. A local attacker can trigger the crash by supplying a malicious input file.	5.5	More Details
CVE-2026-27219	Substance3D - Painter versions 11.1.2 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-28452	OpenClaw versions prior to 2026.2.14 contain a denial of service vulnerability in the extractArchive function within src/infra/archive.ts that allows attackers to consume excessive CPU, memory, and disk resources through high-expansion ZIP and TAR archives. Remote attackers can trigger resource exhaustion by providing maliciously crafted archive files during install or update operations, causing service degradation or system unavailability.	5.5	More Details
CVE-2026-27268	Illustrator versions 29.8.4, 30.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-25180	Out-of-bounds read in Microsoft Graphics Component allows an unauthorized attacker to disclose information locally.	5.5	More Details

CVE-2025-69649	GNU Binutils thru 2.46 readelf contains a null pointer dereference vulnerability when processing a crafted ELF binary with malformed header fields. During relocation processing, an invalid or null section pointer may be passed into display_relocations(), resulting in a segmentation fault (SIGSEGV) and abrupt termination. No evidence of memory corruption beyond the null pointer dereference, nor any possibility of code execution, was observed.	5.5	More Details
CVE-2025-69646	Binutils objdump contains a denial-of-service vulnerability when processing a crafted binary with malformed DWARF debug_rnglists data. A logic error in the handling of the debug_rnglists header can cause objdump to repeatedly print the same warning message and fail to terminate, resulting in an unbounded logging loop until the process is interrupted. The issue was observed in binutils 2.44. A local attacker can exploit this vulnerability by supplying a malicious input file, leading to excessive CPU and I/O usage and preventing completion of the objdump analysis.	5.5	More Details
CVE-2025-69651	GNU Binutils thru 2.46 readelf contains a vulnerability that leads to an invalid pointer free when processing a crafted ELF binary with malformed relocation or symbol data. If dump_relocations returns early due to parsing errors, the internal all_relocations array may remain partially uninitialized. Later, process_got_section_contents() may attempt to free an invalid r_symbol pointer, triggering memory corruption checks in glibc and causing the program to terminate with SIGABRT. No evidence of further memory corruption or code execution was observed; the impact is limited to denial of service.	5.5	More Details
CVE-2026-29780	eml_parser serves as a python module for parsing eml files and returning various information found in the e-mail as well as computed information. Prior to version 2.0.1, the official example script examples/recursively_extract_attachments.py contains a path traversal vulnerability that allows arbitrary file write outside the intended output directory. Attachment filenames extracted from parsed emails are directly used to construct output file paths without any sanitization, allowing an attacker-controlled filename to escape the target directory. This issue has been patched in version 2.0.1.	5.5	More Details
CVE-2026-26949	Dell Device Management Agent (DDMA), versions prior to 26.02, contain an Incorrect Authorization vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	5.5	More Details
CVE-2026-31793	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a segmentation fault due to invalid/wild pointer read in CIccCalculatorFunc::ApplySequence() causing denial of service. This vulnerability is fixed in 2.3.1.5.	5.5	More Details
CVE-2026-30980	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a stack overflow in CIccBasicStructFactory::CreateStruct() causing uncontrolled recursion/stack exhaustion and crash. This vulnerability is fixed in 2.3.1.5.	5.5	More Details
CVE-2026-27270	Illustrator versions 29.8.4, 30.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-24282	Out-of-bounds read in Push Message Routing Service allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-31794	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a segmentation fault from invalid/wild pointer read in CIccCLUT::Interp3d() causing a denial of service. This vulnerability is fixed in 2.3.1.5.	5.5	More Details
CVE-2026-25186	Exposure of sensitive information to an unauthorized actor in Windows Accessibility Infrastructure (ATBroker.exe) allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-30986	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to 2.3.1.5, there is a heap-based buffer overflow write in CIccMatrixMath::SetRange() causing memory corruption or crash. This vulnerability is fixed in 2.3.1.5.	5.5	More Details
CVE-2025-66168	Apache ActiveMQ does not properly validate the remaining length field which may lead to an overflow during the decoding of malformed packets. When this integer overflow occurs, ActiveMQ may incorrectly compute the total Remaining Length and subsequently misinterpret the payload as multiple MQTT control packets which makes the broker susceptible to unexpected behavior when interacting with non-compliant clients. This behavior violates the MQTT v3.1.1 specification, which restricts Remaining Length to a maximum of 4 bytes. The scenario occurs on established connections after the authentication process. Brokers that are not enabling mqtt transport connectors are not impacted. This issue affects Apache ActiveMQ: before 5.19.2, 6.0.0 to 6.1.8, and 6.2.0 Users are recommended to upgrade to version 5.19.2, 6.1.9, or 6.2.1, which fixes the issue.	5.4	More Details

CVE-2026-23808	A vulnerability has been identified in a standardized wireless roaming protocol that could enable a malicious actor to install an attacker-controlled Group Temporal Key (GTK) on a client device. Successful exploitation of this vulnerability could allow a remote malicious actor to perform unauthorized frame injection, bypass client isolation, interfere with cross-client traffic, and compromise network segmentation, integrity, and confidentiality.	5.4	More Details
CVE-2025-70033	An issue pertaining to CWE-79: Improper Neutralization of Input During Web Page Generation was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4.	5.4	More Details
CVE-2026-23601	A vulnerability has been identified in the wireless encryption handling of Wi-Fi transmissions. A malicious actor can generate shared-key authenticated transmissions containing targeted payloads while impersonating the identity of a primary BSSID.Successful exploitation allows for the delivery of tampered data to specific endpoints, bypassing standard cryptographic separation.	5.4	More Details
CVE-2025-64166	Mercurius is a GraphQL adapter for Fastify. Prior to version 16.4.0, a cross-site request forgery (CSRF) vulnerability was identified. The issue arises from incorrect parsing of the Content-Type header in requests. Specifically, requests with Content-Type values such as application/x-www-form-urlencoded, multipart/form-data, or text/plain could be misinterpreted as application/json. This misinterpretation bypasses the preflight checks performed by the fetch() API, potentially allowing unauthorized actions to be performed on behalf of an authenticated user. This issue has been patched in version 16.4.0.	5.4	More Details
CVE-2026-30224	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.11.1, OliveTin does not revoke server-side sessions when a user logs out. Although the browser cookie is cleared, the corresponding session remains valid in server storage until expiry (default ≈ 1 year). An attacker with a previously stolen or captured session cookie can continue authenticating after logout, resulting in a post-logout authentication bypass. This is a session management flaw that violates expected logout semantics. This issue has been patched in version 3000.11.1.	5.4	More Details
CVE-2025-59540	Chamilo is a learning management system. Prior to version 1.11.34, a stored XSS vulnerability exists in Chamilo LMS that allows a staff account to execute arbitrary JavaScript in the browser of higher-privileged admin users. The issue arises because feedback input in the exercise history page is not properly encoded before rendering, allowing malicious scripts to persist in the database and execute on view. This issue has been patched in version 1.11.34.	5.4	More Details
CVE-2026-3103	A logic error in the remove_password() function in Checkmk GmbH's Checkmk versions <2.4.0p23, <2.3.0p43, and 2.2.0 (EOL) allows a low-privileged user to cause data loss.	5.4	More Details
CVE-2026-30964	web-auth/webauthn-lib is an open source set of PHP libraries and a Symfony bundle to allow developers to integrate that authentication mechanism into their web applications. Prior to 5.2.4, when allowed_origins is configured, CheckAllowedOrigins reduces URL-like values to their host component and accepts on host match alone. This makes exact origin policies impossible to express: scheme and port differences are silently ignored. This vulnerability is fixed in 5.2.4.	5.4	More Details
CVE-2025-36226	IBM Aspera Faspex 5 5.0.0 through 5.0.14.3 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2025-36227	IBM Aspera Faspex 5 5.0.0 through 5.0.14.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	5.4	More Details
CVE-2026-23809	A technique has been identified that adapts a known port-stealing method to Wi-Fi environments that use multiple BSSIDs. By leveraging the relationship between BSSIDs and their associated virtual ports, an attacker could potentially bypass inter-BSSID isolation controls. Successful exploitation may enable an attacker to redirect and intercept the victim's network traffic, potentially resulting in eavesdropping, session hijacking, or denial of service.	5.4	More Details
CVE-2026-31832	Umbraco is an ASP.NET CMS. From 14.0.0 to before 16.5.1 and 17.2.2, A broken object-level authorization vulnerability exists in a backoffice API endpoint that allows authenticated users to assign domain-related data to content nodes without proper authorization checks. The issue is caused by insufficient authorization enforcement on the affected API endpoint, whereby via an API call, domains can be set on content nodes that the editor does not have permission to access (either via user group privileges or start nodes). This vulnerability is fixed in 16.5.1 and 17.2.2.	5.4	More Details
CVE-	The Enable Media Replace plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the 'RemoveBackGroundViewController::load' function in all		More

2026-2732	versions up to, and including, 4.1.7. This makes it possible for authenticated attackers, with Author-level access and above, to replace any attachment with a removed background attachment.	5.4	Details
CVE-2026-3761	A flaw has been found in SourceCodester Client Database Management System 1.0. This issue affects some unknown processing of the file /superadmin_user_delete.php of the component Endpoint. Executing a manipulation of the argument user_id can lead to improper authorization. The attack may be performed from remote. The exploit has been published and may be used.	5.4	More Details
CVE-2025-70060	An issue pertaining to CWE-79: Improper Neutralization of Input During Web Page Generation was discovered in YMFE yapi v1.12.0.	5.4	More Details
CVE-2025-13213	IBM Aspera Orchestrator 3.0.0 through 4.1.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking	5.4	More Details
CVE-2026-29061	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to version 2.2.3, a privilege escalation vulnerability in the user rank demotion logic allows a demoted user's existing API keys to retain ApiPermManageFileRequests and ApiPermManageLogs permissions, enabling continued access to upload-request management and log viewing endpoints after the user has been stripped of all privileges. This issue has been patched in version 2.2.3.	5.4	More Details
CVE-2026-26377	Cross Site Scripting vulnerability in Koha 25.11 and before allows a remote attacker to execute arbitrary code via the News function.	5.4	More Details
CVE-2026-27898	Vaultwarden is an unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. Prior to version 1.35.4, an authenticated regular user can specify another user’s cipher_id and call "PUT /api/ciphers/{id}/partial" Even though the standard retrieval API correctly denies access to that cipher, the partial update endpoint returns 200 OK and exposes cipherDetails (including name, notes, data, secureNote, etc.). This issue has been patched in version 1.35.4.	5.4	More Details
CVE-2026-25604	In AWS Auth manager, the origin of the SAML authentication has been used as provided by the client and not verified against the actual instance URL. This allowed to gain access to different instances with potentially different access controls by reusing SAML response from other instances. You should upgrade to 9.22.0 version of provider if you use AWS Auth Manager.	5.4	More Details
CVE-2026-29086	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.12.4, the setCookie() utility did not validate semicolons (;), carriage returns (\r), or newline characters (\n) in the domain and path options when constructing the Set-Cookie header. Because cookie attributes are delimited by semicolons, this could allow injection of additional cookie attributes if untrusted input was passed into these fields. This issue has been patched in version 4.12.4.	5.4	More Details
CVE-2026-3817	A vulnerability was detected in SourceCodester Patients Waiting Area Queue Management System 1.0. This issue affects some unknown processing of the file /patient-search.php. The manipulation results in improper authorization. The attack can be launched remotely. The exploit is now public and may be used.	5.3	More Details
CVE-2026-31825	Sylius is an Open Source eCommerce Framework on Symfony. Sylius API filters ProductPriceOrderFilter and TranslationOrderNameAndLocaleFilter pass user-supplied order direction values directly to Doctrine's orderBy() without validation. An attacker can inject arbitrary DQL. The issue is fixed in versions: 1.9.12, 1.10.16, 1.11.17, 1.12.23, 1.13.15, 1.14.18, 2.0.16, 2.1.12, 2.2.3 and above.	5.3	More Details
CVE-2026-27796	Homarr is an open-source dashboard. Prior to version 1.54.0, the integration.all tRPC endpoint in Homarr is exposed as a publicProcedure, allowing unauthenticated users to retrieve a complete list of configured integrations. This metadata includes sensitive information such as internal service URLs, integration names, and service types. This issue has been patched in version 1.54.0.	5.3	More Details
CVE-2026-27445	SEPPmail Secure Email Gateway before version 15.0.1 does not properly verify that a PGP signature was generated by the expected key, allowing signature spoofing.	5.3	More Details
CVE-2026-26309	Envoy is a high-performance edge/middle/service proxy. Prior to 1.37.1, 1.36.5, 1.35.8, and 1.34.13, an off-by-one write in Envoy::JsonEscaper::escapeString() can corrupt std::string null-termination, causing undefined behavior and potentially leading to crashes or out-of-bounds reads when the resulting string is later treated as a C-string. This vulnerability is fixed in 1.37.1, 1.36.5, 1.35.8, and 1.34.13.	5.3	More Details
	OpenClaw version 2026.1.14-1 prior to 2026.2.2, with the Matrix plugin installed and enabled, contain		

CVE-2026-28471	a vulnerability in which DM allowlist matching could be bypassed by exact-matching against sender display names and localparts without homeserver validation. Remote Matrix users can impersonate allowed identities by using attacker-controlled display names or matching localparts from different homeservers to reach the routing and agent pipeline.	5.3	More Details
CVE-2026-2746	SEPPmail Secure Email Gateway before version 15.0.1 does not properly communicate PGP signature verification results, leaving users unable to detect forged emails.	5.3	More Details
CVE-2025-70040	An issue pertaining to CWE-532: Insertion of Sensitive Information into Log File was discovered in LupinLin1 jimeng-web-mcp v2.1.2. This allows an attacker to obtain sensitive information.	5.3	More Details
CVE-2026-26330	Envoy is a high-performance edge/middle/service proxy. Prior to 1.37.1, 1.36.5, 1.35.8, and 1.34.13, At the rate limit filter, if the response phase limit with apply_on_stream_done in the rate limit configuration is enabled and the response phase limit request fails directly, it may crash Envoy. When both the request phase limit and response phase limit are enabled, the safe gRPC client instance will be re-used for both the request phase request and response phase request. But after the request phase request is done, the inner state of the request phase limit request in gRPC client is not cleaned up. When a second limit request is sent at response phase, and the second limit request fails directly, the previous request's inner state may be accessed and result in crash. This vulnerability is fixed in 1.37.1, 1.36.5, 1.35.8, and 1.34.13.	5.3	More Details
CVE-2018-25174	ABC ERP 0.6.4 contains a cross-site request forgery vulnerability that allows attackers to modify administrator credentials by submitting forged requests to _configurar_perfil.php. Attackers can craft malicious forms or links containing parameters like usuario, contrasena1, contrasena2, nombre, and email to change admin account settings without authentication.	5.3	More Details
CVE-2026-2748	SEPPmail Secure Email Gateway before version 15.0.1 improperly validates S/MIME certificates issued for email addresses containing whitespaces, allowing signature spoofing.	5.3	More Details
CVE-2026-28687	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a heap use-after-free vulnerability in ImageMagick's MSL decoder allows an attacker to trigger access to freed memory by crafting an MSL file. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	5.3	More Details
CVE-2026-1650	The MDJM Event Management plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the 'custom_fields_controller' function in all versions up to, and including, 1.7.8.1. This makes it possible for unauthenticated attackers to delete arbitrary custom event fields via the 'delete_custom_field' and 'id' parameters.	5.3	More Details
CVE-2026-25907	Dell PowerScale OneFS, version 9.13.0.0, contains an overly restrictive account lockout mechanism vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	5.3	More Details
CVE-2026-29069	Craft is a content management system (CMS). Prior to 5.9.0-beta.2 and 4.17.0-beta.2, the actionSendActivationEmail() endpoint is accessible to unauthenticated users and does not require a permission check for pending users. An attacker with no prior access can trigger activation emails for any pending user account by knowing or guessing the user ID. If the attacker controls the target user's email address, they can activate the account and gain access to the system. This vulnerability is fixed in 5.9.0-beta.2 and 4.17.0-beta.2.	5.3	More Details
CVE-2026-1980	The WPBookit plugin for WordPress is vulnerable to unauthorized data disclosure due to a missing authorization check on the 'get_customer_list' route in all versions up to, and including, 1.0.8. This makes it possible for unauthenticated attackers to retrieve sensitive customer information including names, emails, phone numbers, dates of birth, and gender.	5.3	More Details
CVE-2026-28428	Talishar is a fan-made Flesh and Blood project. Prior to commit a9c218e, an authentication bypass vulnerability in Talishar's game endpoint validation logic allows any unauthenticated attacker to perform authenticated game actions — including sending chat messages and submitting game inputs — by supplying an empty authKey parameter (authKey=). The server-side validation uses a loose comparison that accepts an empty string as a valid credential, while correctly rejecting non-empty but incorrect keys. This asymmetry means the authentication mechanism can be completely bypassed without knowing any valid token. This issue has been patched in commit a9c218e.	5.3	More Details
	A vulnerability in the implementation of the proprietary SSH stack with SSH key-based authentication in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to log in to a Cisco Secure Firewall ASA device and execute commands as a specific		

CVE-2026-20009	user. This vulnerability is due to insufficient validation of user input during the SSH authentication phase. An attacker could exploit this vulnerability by submitting crafted input during SSH authentication to an affected device. A successful exploit could allow the attacker to log in to the device as a specific user without the private SSH key of that user. To exploit this vulnerability, the attacker must possess a valid username and the associated public key. The private key is not required. Notes: Exploitation of this vulnerability does not provide the attacker with root access. The authentication, authorization, and accounting (AAA) configuration command auto-enable is not affected by this vulnerability.&nbsp;&nbsp;	5.3	More Details
CVE-2026-25185	Exposure of sensitive information to an unauthorized actor in Windows Shell Link Processing allows an unauthorized attacker to perform spoofing over a network.	5.3	More Details
CVE-2026-30225	OliveTin gives access to predefined shell commands from a web interface. Prior to version 3000.11.1, an authentication context confusion vulnerability in RestartAction allows a low-privileged authenticated user to execute actions they are not permitted to run. RestartAction constructs a new internal connect.Request without preserving the original caller's authentication headers or cookies. When this synthetic request is passed to StartAction, the authentication resolver falls back to the guest user. If the guest account has broader permissions than the authenticated caller, this results in privilege escalation and unauthorized command execution. This vulnerability allows a low-privileged authenticated user to bypass ACL restrictions and execute arbitrary configured shell actions. This issue has been patched in version 3000.11.1.	5.3	More Details
CVE-2026-28675	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Prior to version 1.6.3-alpha, some endpoints returned raw exception strings to clients. Additionally, login token material was exposed in UI/rendered responses and token rotation output. This issue has been patched in version 1.6.3-alpha.	5.3	More Details
CVE-2026-20031	A vulnerability in the HTML Cascading Style Sheets (CSS) module of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling when splitting UTF-8 strings. An attacker could exploit this vulnerability by submitting a crafted HTML file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the scanning process.	5.3	More Details
CVE-2026-23907	This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.35, from 3.0.0 through 3.0.6. The ExtractEmbeddedFiles example contains a path traversal vulnerability (CWE-22) because the filename that is obtained from PDComplexFileSpecification.getFilename() is appended to the extraction path. Users who have copied this example into their production code should review it to ensure that the extraction path is acceptable. The example has been changed accordingly, now the initial path and the extraction paths are converted into canonical paths and it is verified that extraction path contains the initial path. The documentation has also been adjusted.	5.3	More Details
CVE-2026-20106	A vulnerability in the Remote Access SSL VPN, HTTP management and MUS functionality, of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to exhaust device memory resulting in a denial of service (DoS) condition requiring a manual reboot. This vulnerability is due to trusting user input without validation. An attacker could exploit this vulnerability by sending crafted packets to the Remote Access SSL VPN server. A successful exploit could allow the attacker to cause the device to stop responding, resulting in a DoS condition.	5.3	More Details
CVE-2026-28804	pypdf is a free and open-source pure-python PDF library. Prior to version 6.7.5, an attacker who uses this vulnerability can craft a PDF which leads to long runtimes. This requires accessing a stream which uses the /ASCIIHexDecode filter. This issue has been patched in version 6.7.5.	5.3	More Details
CVE-2026-22628	An improper access control vulnerability in Fortinet FortiSwitchAXFixed 1.0.0 through 1.0.1 may allow an authenticated admin to execute system commands via a specifically crafted SSH config file.	5.3	More Details
CVE-2026-28434	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.35.0, when a request handler throws a C++ exception and the application has not registered a custom exception handler via set_exception_handler(), the library catches the exception and writes its message directly into the HTTP response as a header named EXCEPTION_WHAT. This header is sent to whoever made the request, with no authentication check and no special configuration required to trigger it. The behavior is on by default. A developer who does not know to opt in to set_exception_handler() will ship a server that leaks internal exception messages to any client. This vulnerability is fixed in 0.35.0.	5.3	More Details
CVE-2026-	Homarr is an open-source dashboard. Prior to version 1.54.0, an unauthenticated Server-Side Request Forgery (SSRF) vulnerability allows a remote attacker to force the Homarr server to perform arbitrary outbound HTTP requests. This can be used as an internal network access primitive (e.g., reaching	5.3	More

27797	loopback/private ranges) from the Homarr host/container network context. This issue has been patched in version 1.54.0.		Details
CVE-2025-48840	An authentication bypass by spoofing vulnerability in Fortinet FortiWeb 7.6.0 through 7.6.3, FortiWeb 7.4.0 through 7.4.8, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow a remote unauthenticated attacker to bypass hostname restrictions via a specially crafted request.	5.3	More Details
CVE-2025-41711	An unauthenticated remote attacker can use firmware images to extract password hashes and brute force plaintext passwords of accounts with limited access.	5.3	More Details
CVE-2026-2371	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 12.8.3. This is due to missing authorization and post status validation in the `gspb_el_reusable_load()` AJAX handler. The handler accepts an arbitrary `post_id` parameter and renders the content of any `wp_block` post without checking `current_user_can('read_post', $post_id)` or verifying the post status. Combined with the nonce being exposed to unauthenticated users on any public page using the `[wp_reusable_render]` shortcode with `ajax="1"`, this makes it possible for unauthenticated attackers to retrieve the rendered HTML content of private, draft, or password-protected reusable blocks.	5.3	More Details
CVE-2026-2589	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 12.8.3 via the automated Settings Backup stored in a publicly accessible file. This makes it possible for unauthenticated attackers to extract sensitive data including the configured OpenAI, Claude, Google Maps, Gemini, DeepSeek, and Cloudflare Turnstile API keys.	5.3	More Details
CVE-2026-1920	The Booking Calendar for Appointments and Service Businesses – Booktics plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'Extension_Controller::update_item_permissions_check' function in all versions up to, and including, 1.0.16. This makes it possible for unauthenticated attackers to install addon plugins.	5.3	More Details
CVE-2026-1919	The Booking Calendar for Appointments and Service Businesses – Booktics plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on multiple REST API endpoints in all versions up to, and including, 1.0.16. This makes it possible for unauthenticated attackers to query sensitive data.	5.3	More Details
CVE-2026-22040	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. In version 0.24.6, by generating a combined traffic pattern of high-frequency publishes and rapid reconnect/kick-out using the same ClientID and massive subscribe/unsubscribe jitter, it is possible to reliably trigger heap memory corruption in the Broker process, causing it to exit immediately with SIGABRT due to free(): invalid pointer. As of time of publication, no known patched versions are available.	5.3	More Details
CVE-2018-25177	Data Center Audit 2.6.2 contains a cross-site request forgery vulnerability that allows attackers to reset administrator passwords without authentication by submitting crafted POST requests. Attackers can send requests to dca_resetpw.php with parameters updateuser, pass, pass2, and submit_reset to change the admin account password and gain administrative access.	5.3	More Details
CVE-2026-27411	Guessable CAPTCHA vulnerability in jp-secure SiteGuard WP Plugin siteguard allows Functionality Bypass.This issue affects SiteGuard WP Plugin: from n/a through <= 1.7.9.	5.3	More Details
CVE-2026-3713	A flaw has been found in pnggroup libpng up to 1.6.55. Affected by this vulnerability is the function do_pnm2png of the file contrib/pngminus/pnm2png.c of the component pnm2png. This manipulation of the argument width/height causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-3675	A vulnerability was determined in Freedom Factory dGEN1 up to 20260221. Affected by this issue is the function FakeAppReceiver of the component org.ethosmobile.ethoslauncher. Executing a manipulation can lead to improper authorization. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2018-25200	OOP CMS BLOG 1.0 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to create administrative user accounts by crafting malicious POST requests. Attackers can submit forms to the addUser.php endpoint with parameters including userName, password, email, and role set to administrative privileges to gain unauthorized access.	5.3	More Details
	A vulnerability was found in Freedom Factory dGEN1 up to 20260221. Affected by this vulnerability is		

CVE-2026-3674	the function FakeAppProvider of the component org.ethosmobile.ethoslauncher. Performing a manipulation results in improper authorization. The attack must be initiated from a local position. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-31808	file-type detects the file type of a file, stream, or data. Prior to 21.3.1, a denial of service vulnerability exists in the ASF (WMV/WMA) file type detection parser. When parsing a crafted input where an ASF sub-header has a size field of zero, the parser enters an infinite loop. The payload value becomes negative (-24), causing tokenizer.ignore(payload) to move the read position backwards, so the same sub-header is read repeatedly forever. Any application that uses file-type to detect the type of untrusted/attacker-controlled input is affected. An attacker can stall the Node.js event loop with a 55-byte payload. Fixed in version 21.3.1.	5.3	More Details
CVE-2026-3670	A vulnerability was detected in Freedom Factory dGEN1 up to 20260221. Affected is an unknown function of the component com.dgen.alarm. Performing a manipulation results in improper authorization. The attack requires a local approach. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-3669	A security vulnerability has been detected in Freedom Factory dGEN1 up to 20260221. This impacts the function AlarmService of the component com.dgen.alarm. Such manipulation leads to improper authorization. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-30859	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.12, a broken access control vulnerability in the database query tool allows any authenticated tenant to read sensitive data belonging to other tenants, including API keys, model configurations, and private messages. The application fails to enforce tenant isolation on critical tables (models, messages, embeddings), enabling unauthorized cross-tenant data access with user-level authentication privileges. This issue has been patched in version 0.2.12.	5.3	More Details
CVE-2026-3707	A vulnerability was identified in MrNanko webp4j up to 1.3.x. The affected element is the function DecodeGifFromMemory of the file src/main/c/gif_decoder.c. Such manipulation of the argument canvas_height leads to integer overflow. Local access is required to approach this attack. The exploit is publicly available and might be used. The name of the patch is 89771b201c66d15d29e4cc016d8aae82b6a5fbe1. It is advisable to implement a patch to correct this issue.	5.3	More Details
CVE-2026-30829	Checkmate is an open-source, self-hosted tool designed to track and monitor server hardware, uptime, response times, and incidents in real-time with beautiful visualizations. Prior to version 3.4.0, an unauthenticated information disclosure vulnerability exists in the GET /api/v1/status-page/:url endpoint. The endpoint does not enforce authentication or verify whether a status page is published before returning full status page details. As a result, unpublished status pages and their associated internal data are accessible to any unauthenticated user via direct API requests. This issue has been patched in version 3.4.0.	5.3	More Details
CVE-2026-28413	Products.isurlinportal is a replacement for isURLInPortal method in Plone. Prior to versions 2.1.0, 3.1.0, and 4.0.0, a url /login?came_from=////evil.example may redirect to an external website after login. This issue has been patched in versions 2.1.0, 3.1.0, and 4.0.0.	5.3	More Details
CVE-2026-30854	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. From version 9.3.1-alpha.3 to before version 9.5.0-alpha.10, when graphQLPublicIntrospection is disabled, __type queries nested inside inline fragments (e.g. ... on Query { __type(name:"User") { name } }) bypass the introspection control, allowing unauthenticated users to perform type reconnaissance. __schema introspection is not affected. This issue has been patched in version 9.5.0-alpha.10.	5.3	More Details
CVE-2026-3667	A security flaw has been discovered in Freedom Factory dGEN1 up to 20260221. The impacted element is the function FakeAppService of the component org.ethosmobile.ethoslauncher. The manipulation results in improper authorization. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-31815	Unicorn adds modern reactive component functionality to your Django templates. Prior to 0.67.0, component state manipulation is possible in django-unicorn due to missing access control checks during property updates and method calls. An attacker can bypass the intended _is_public protection to modify internal attributes such as template_name or trigger protected methods. This vulnerability is fixed in 0.67.0.	5.3	More Details
	Navtor NavBox allows information disclosure via the /api/ais-data endpoint. A remote, unauthenticated		

CVE-2026-2752	attacker can send crafted requests to trigger an unhandled exception, causing the server to return verbose .NET stack traces. These error messages expose internal class names, method calls, and third-party library references (e.g., System.Data.SQLite), which may assist attackers in mapping the application's internal structure.	5.3	More Details
CVE-2026-30857	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.3.0, a cross-tenant authorization bypass in the knowledge base copy endpoint allows any authenticated user to clone (duplicate) another tenant’s knowledge base into their own tenant by knowing/guessing the source knowledge base ID. This enables bulk data exfiltration (document/FAQ content) across tenants. This issue has been patched in version 0.3.0.	5.3	More Details
CVE-2026-3719	A vulnerability was identified in Tsinghua Unigroup Electronic Archives System 3.2.210802(62532). This issue affects some unknown processing of the file /System/Cms/downLoad. The manipulation of the argument path leads to path traversal. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2018-25186	Tina4 Stack 1.0.3 contains a cross-site request forgery vulnerability that allows attackers to modify admin user credentials by submitting forged POST requests to the profile endpoint. Attackers can craft HTML forms targeting the /kim/profile endpoint with hidden fields containing malicious user data like passwords and email addresses to update administrator accounts without authentication.	5.3	More Details
CVE-2026-3731	A weakness has been identified in libssh up to 0.11.3. The impacted element is the function sftp_extensions_get_name/sftp_extensions_get_data of the file src/sftp.c of the component SFTP Extension Name Handler. Executing a manipulation of the argument idx can lead to out-of-bounds read. The attack may be performed from remote. Upgrading to version 0.11.4 and 0.12.0 is sufficient to resolve this issue. This patch is called 855a0853ad3abd4a6cd85ce06fce6d8d4c7a0b60. You should upgrade the affected component.	5.3	More Details
CVE-2026-29787	mcp-memory-service is an open-source memory backend for multi-agent systems. Prior to version 10.21.0, the /api/health/detailed endpoint returns detailed system information including OS version, Python version, CPU count, memory totals, disk usage, and the full database filesystem path. When MCP_ALLOW_ANONYMOUS_ACCESS=true is set (required for the HTTP server to function without OAuth/API key), this endpoint is accessible without authentication. Combined with the default 0.0.0.0 binding, this exposes sensitive reconnaissance data to the entire network. This issue has been patched in version 10.21.0.	5.3	More Details
CVE-2026-3796	A weakness has been identified in Qi-ANXIN QAX Virus Removal up to 2025-10-22. The affected element is the function ZwTerminateProcess in the library QKSecureIO_Imp.sys of the component Mini Filter Driver. Executing a manipulation can lead to improper access controls. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-27344	Missing Authorization vulnerability in inseriswiss inseri core inseri-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects inseri core: from n/a through <= 1.0.5.	5.3	More Details
CVE-2018-25190	Easyndexer 1.0 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to create administrative accounts by submitting forged POST requests. Attackers can craft malicious web pages that submit POST requests to createuser.php with parameters including username, password, name, surname, and privileges set to 1 for administrator access.	5.3	More Details
CVE-2026-3419	Fastify incorrectly accepts malformed \`Content-Type\` headers containing trailing characters after the subtype token, in violation of RFC 9110 §8.3.1(https://httpwg.org/specs/rfc9110.html#field.content-type). For example, a request sent with Content-Type: application/json garbage passes validation and is processed normally, rather than being rejected with 415 Unsupported Media Type. When regex-based content-type parsers are in use (a documented Fastify feature), the malformed value is matched against registered parsers using the full string including the trailing garbage. This means a request with an invalid content-type may be routed to and processed by a parser it should never have reached. Impact: An attacker can send requests with RFC-invalid Content-Type headers that bypass validity checks, reach content-type parser matching, and be processed by the server. Requests that should be rejected at the validation stage are instead handled as if the content-type were valid. Workarounds: Deploy a WAF rule to protect against this Fix: The fix is available starting with v5.8.1.	5.3	More Details
CVE-2026-26196	Gogs is an open source self-hosted Git service. Prior to version 0.14.2, gogs api still accepts tokens in url params like token and access_token, which can leak through logs, browser history, and referrers. This issue has been patched in version 0.14.2.	5.3	More Details
CVE-	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). The SICAM SIAPP SDK		

2026-25571	client component does not enforce maximum length checks on certain variables before use. This could allow an attacker to send an oversized input that could trigger a stack overflow crashing the process and potentially causing denial of service.	5.1	More Details
CVE-2026-28537	Double free vulnerability in the window module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2026-25572	A vulnerability has been identified in SICAM SIAPP SDK (All versions < V2.1.7). The SICAM SIAPP SDK server component does not enforce maximum length checks on certain variables before use. This could allow an attacker to send an oversized input that could trigger a stack overflow crashing the process and potentially causing denial of service.	5.1	More Details
CVE-2026-24317	SAP GUI for Windows allows DLL files to be loaded from arbitrary directories within the application. An unauthenticated attacker could exploit this vulnerability by persuading a victim to place a malicious DLL within one of these directories. The malicious command is executed in the victim user's context provided GuiXT is enabled. This vulnerability has a low impact on confidentiality, integrity, and availability.	5.0	More Details
CVE-2026-27688	Due to a missing authorization check in SAP NetWeaver Application Server for ABAP, an authenticated attacker with user privileges could read Database Analyzer Log Files via a specific RFC function module. The attacker with the necessary privileges to execute this function module could potentially escalate their privileges and read the sensitive data, resulting in a limited impact on the confidentiality of the information stored. However, the integrity and availability of the system are not affected.	5.0	More Details
CVE-2026-29060	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to version 2.2.3, a registered user without privileges to create or modify file requests is able to create a short-lived API key that has the permission to do so. The user must be registered with Gokapi. If there are no users with access to the admin/upload menu, there is no impact. This issue has been patched in version 2.2.3.	5.0	More Details
CVE-2026-27023	Twenty is an open source CRM. Prior to version 1.18, the SSRF protection in SecureHttpClientService validated request URLs at the request level but did not validate redirect targets. An authenticated user who could control outbound request URLs (e.g., webhook endpoints, image URLs) could bypass private IP blocking by redirecting through an attacker-controlled server. This issue has been patched in version 1.18.	5.0	More Details
CVE-2025-69644	An issue was discovered in Binutils before 2.46. The objdump contains a denial-of-service vulnerability when processing a crafted binary with malformed debug information. A logic flaw in the handling of DWARF location list headers can cause objdump to enter an unbounded loop and produce endless output until manually interrupted. This issue affects versions prior to the upstream fix and allows a local attacker to cause excessive resource consumption by supplying a malicious input file.	5.0	More Details
CVE-2026-24313	SAP Solution Tools Plug-In (ST-PI) contains a function module that does not perform the necessary authorization checks for authenticated users, allowing system information to be disclosed. This vulnerability has a low impact on confidentiality and does not affect integrity or availability.	5.0	More Details
CVE-2026-2429	The Community Events plugin for WordPress is vulnerable to SQL Injection via the 'ce_venue_name' CSV field in the `on_save_changes_venues` function in all versions up to, and including, 1.5.8. This is due to insufficient escaping on the user-supplied CSV data and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database via a crafted CSV file upload.	4.9	More Details
CVE-2026-29791	Agentgateway is an open source data plane for agentic AI connectivity within or across any agent framework or environment. Prior to version 0.12.0, when converting MCP tools/call request to OpenAPI request, input path, query, and header values are not sanitized. This issue has been patched in version 0.12.0.	4.9	More Details
CVE-2026-3523	The Apocalypse Meow plugin for WordPress is vulnerable to SQL Injection via the 'type' parameter in all versions up to, and including, 22.1.0. This is due to a flawed logical operator in the type validation check on line 261 of ajax.php — the condition uses `&&` (AND) instead of `||` (OR), causing the `in_array()` validation to be short-circuited and never evaluated for any non-empty type value. Combined with `stripslashes_deep()` being called on line 101 which removes `wp_magic_quotes()` protection, attacker-controlled single quotes pass through unescaped into the SQL query on line 298. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details

CVE-2026-3439	A post-authentication Stack-based Buffer Overflow vulnerability in SonicOS certificate handling allows a remote attacker to crash a firewall.	4.9	More Details
CVE-2026-27807	MarkUs is a web application for the submission and grading of student assignments. Prior to version 2.9.4, MarkUs allows course instructors to upload YAML files to create/update various entities (e.g., assignment settings). These YAML files are parsed with aliases enabled. This issue has been patched in version 2.9.4.	4.9	More Details
CVE-2025-41760	An administrator may attempt to block all traffic by configuring a pass filter with an empty table. However, in UBR, an empty list does not enforce any restrictions and allows all network traffic to pass unfiltered.	4.9	More Details
CVE-2026-20003	A vulnerability in the REST API of Cisco Secure FMC Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to inadequate validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted requests to an affected device. A successful exploit could allow the attacker to obtain read access to the database and read certain files on the underlying operating system. To exploit this vulnerability, the attacker would need valid user credentials with any of the following roles: Administrator Security approver Intrusion admin Access admin Network admin	4.9	More Details
CVE-2025-41759	An administrator may attempt to block all networks by specifying "*" or "all" as the network identifier. However, these values are not supported and do not trigger any validation error. Instead, they are silently interpreted as network 0 which results in no networks being blocked at all.	4.9	More Details
CVE-2026-28078	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Stylemix uListing ulisting allows Path Traversal.This issue affects uListing: from n/a through <= 2.2.0.	4.9	More Details
CVE-2026-3241	In Concrete CMS below version 9.4.8, a stored cross-site scripting (XSS) vulnerability exists in the "Legacy Form" block. An authenticated user with permissions to create or edit forms (e.g., a rogue administrator) can inject a persistent JavaScript payload into the options of a multiple-choice question (Checkbox List, Radio Buttons, or Select Box). This payload is then executed in the browser of any user who views the page containing the form. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks M3dium for reporting.	4.8	More Details
CVE-2026-3242	In Concrete CMS below version 9.4.8, a rogue administrator can add stored XSS via the Switch Language block. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks M3dium for reporting.	4.8	More Details
CVE-2025-70973	ScadaBR 1.12.4 is vulnerable to Session Fixation. The application assigns a JSESSIONID session cookie to unauthenticated users and does not regenerate the session identifier after successful authentication. As a result, a session created prior to login becomes authenticated once the victim logs in, allowing an attacker who knows the session ID to hijack an authenticated session.	4.8	More Details
CVE-2026-28692	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, MAT decoder uses 32-bit arithmetic due to incorrect parenthesization resulting in a heap over-read. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	4.8	More Details
CVE-2026-28475	OpenClaw versions prior to 2026.2.13 use non-constant-time string comparison for hook token validation, allowing attackers to infer tokens through timing measurements. Remote attackers with network access to the hooks endpoint can exploit timing side-channels across multiple requests to gradually recover the authentication token.	4.8	More Details
CVE-2026-2722	The Stock Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.26.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.8	More Details
CVE-2026-2721	The MailArchiver plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.8	More Details
CVE-	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability		

2025-53608	[CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an authenticated privileged attacker to execute code via crafted requests.	4.8	More Details
CVE-2025-40895	A Stored HTML Injection vulnerability was discovered in the CMC's Sensor Map functionality due to improper validation on connected Guardians' properties. A malicious authenticated user with administrator privileges on a Guardian connected to a CMC can edit the Guardian's properties to inject HTML tags. If the Sensor Map functionality is enabled in the CMC, when a victim CMC user interacts with it, then the injected HTML may render in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	4.8	More Details
CVE-2026-3244	In Concrete CMS below version 9.4.8, A stored cross-site scripting (XSS) vulnerability exists in the search block where page names and content are rendered without proper HTML encoding in search results. This allows authenticated, rogue administrators to inject malicious JavaScript through page names that executes when users search for and view those pages in search results. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks zolpak for reporting	4.8	More Details
CVE-2026-3240	In Concrete CMS below version 9.4.8, a user with permission to edit a page with element Legacy form can perform a stored XSS attack towards high-privilege accounts via the Question field. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Thanks minhnn42, namdi and quanlna2 from VCSLab-Viettel Cyber Security for reporting.	4.8	More Details
CVE-2026-31823	Sylius is an Open Source eCommerce Framework on Symfony. An authenticated stored cross-site scripting (XSS) vulnerability exists in multiple places across the shop frontend and admin panel due to unsanitized entity names being rendered as raw HTML. Shop breadcrumbs (shared/breadcrumbs.html.twig): The breadcrumbs macro uses the Twig |raw filter on label values. Since taxon names, product names, and ancestor names flow directly into these labels, a malicious taxon name like <img src=x onerror=alert('XSS')> is rendered and executed as JavaScript on the storefront. Admin product taxon picker (ProductTaxonTreeController.js): The rowRenderer method interpolates ${name} directly into a template literal building HTML, allowing script injection through taxon names in the admin panel. Admin autocomplete fields (Tom Select): Dropdown items and options render entity names as raw HTML without escaping, allowing XSS through any autocomplete field displaying entity names. An authenticated administrator can inject arbitrary HTML or JavaScript via entity names (e.g. taxon name) that is persistently rendered for all users. The issue is fixed in versions: 1.9.12, 1.10.16, 1.11.17, 1.12.23, 1.13.15, 1.14.18, 2.0.16, 2.1.12, 2.2.3 and above.	4.8	More Details
CVE-2025-41257	Suprema’s BioStar 2 in version 2.9.11.6 allows users to set new password without providing the current one. Exploiting this flaw combined with other vulnerabilities can lead to unauthorized account access and potential system compromise.	4.8	More Details
CVE-2026-3711	A vulnerability was detected in code-projects Simple Flight Ticket Booking System 1.0. Affected is an unknown function of the file /Adminupdate.php. The manipulation of the argument flightno/airplaneid/departure/dtime/arrival/atime/ec/ep/bc/bp results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2026-3714	A vulnerability has been found in OpenCart 4.0.2.3. Affected by this issue is the function Save of the file admin/controller/design/template.php of the component Incomplete Fix CVE-2024-36694. Such manipulation leads to improper neutralization of special elements used in a template engine. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-28106	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Kings Plugins B2BKing Premium allows Phishing.This issue affects B2BKing Premium: from n/a before 5.4.20.	4.7	More Details
CVE-2026-3704	A vulnerability has been found in Wavlink NU516U1 251208. This vulnerability affects the function sub_405B2C of the file /cgi-bin/firewall.cgi of the component Incomplete Fix CVE-2025-10959. The manipulation leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	4.7	More Details
CVE-2026-3710	A security vulnerability has been detected in code-projects Simple Flight Ticket Booking System 1.0. This impacts an unknown function of the file /Adminadd.php. The manipulation of the argument flightno/airplaneid/departure/dtime/arrival/atime/ec/ep/bc/bp leads to sql injection. Remote	4.7	More Details

	exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.		
CVE-2026-3750	A security vulnerability has been detected in ContiNew Admin up to 4.2.0. This issue affects the function URI.create of the file continew-system/src/main/java/top/continew/admin/system/factory/S3ClientFactory.java of the component Storage Management Module. The manipulation leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-3751	A vulnerability was detected in SourceCodester Employee Task Management System 1.0. Impacted is an unknown function of the file /daily-attendance-report.php of the component GET Parameter Handler. The manipulation of the argument Date results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	4.7	More Details
CVE-2026-3752	A flaw has been found in SourceCodester Employee Task Management System up to 1.0. The affected element is an unknown function of the file /daily-task-report.php of the component GET Parameter Handler. This manipulation of the argument Date causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2026-3798	A vulnerability was detected in Comfast CF-AC100 2.6.0.8. This affects the function sub_44AC14 of the file /cgi-bin/mbox-config?method=SET&section=ping_config of the component Request Path Handler. The manipulation results in command injection. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-3662	A vulnerability has been found in Wavlink WL-NU516U1 240425. This vulnerability affects the function usb_p910 of the file /cgi-bin/adm.cgi. Such manipulation of the argument Pr_mode leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	4.7	More Details
CVE-2026-28551	Race condition vulnerability in the device security management module. Impact: Successful exploitation of this vulnerability may affect availability.	4.7	More Details
CVE-2026-3661	A flaw has been found in Wavlink WL-NU516U1 240425. This affects the function ota_new_upgrade of the file /cgi-bin/adm.cgi. This manipulation of the argument model causes command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	4.7	More Details
CVE-2026-30974	Copyparty is a portable file server. Prior to v1.20.11., the nohtml config option, intended to prevent execution of JavaScript in user-uploaded HTML files, did not apply to SVG images. A user with write-permission could upload an SVG containing embedded JavaScript, which would execute in the context of whichever user opens it. This has been fixed in v1.20.11.	4.6	More Details
CVE-2026-30913	Flarum is open-source forum software. When the flarum/nicknames extension is enabled, a registered user can set their nickname to a string that email clients interpret as a hyperlink. The nickname is inserted verbatim into plain-text notification emails, and recipients may be misled into visiting attacker-controlled domains.	4.6	More Details
CVE-2026-29084	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. Prior to version 2.2.3, the login flow accepts credential-bearing requests without CSRF protection mechanisms tied to the browser session context. The handler parses form values directly and creates a session on successful credential validation. This issue has been patched in version 2.2.3.	4.6	More Details
CVE-2026-2289	The Taskbuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 5.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-30935	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16, BilateralBlurImage contains a heap buffer over-read caused by an incorrect conversion. When processing a crafted image with the -bilateral-blur operation an out of bounds read can occur. This vulnerability is fixed in 7.1.2-16.	4.4	More Details
CVE-2026-21736	Software installed and run as a non-privileged user may conduct improper GPU system calls to gain write permission to read-only wrapped user-mode memory. This is caused by improper handling of the memory protections for the user-mode wrapped memory resource.	4.4	More Details

CVE-2026-22285	Dell Device Management Agent (DDMA), versions prior to 26.02, contain a Plaintext Storage of Password vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized Access.	4.4	More Details
CVE-2025-40894	A Stored HTML Injection vulnerability was discovered in the Alerted Nodes Dashboard functionality due to improper validation on an input parameter. A malicious authenticated user with the required privileges could edit a node label to inject HTML tags. If the system is configured to use the Alerted Nodes Dashboard, and alerts are reported for the affected node, then the injected HTML may render in the browser of a victim user interacting with it, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	4.4	More Details
CVE-2026-2292	The Morkva UA Shipping plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.7.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-26998	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.38 and 3.6.9, there is a potential vulnerability in Traefik managing the ForwardAuth middleware responses. When Traefik is configured to use the ForwardAuth middleware, the response body from the authentication server is read entirely into memory without any size limit. There is no maxResponseBodySize configuration to restrict the amount of data read from the authentication server response. If the authentication server returns an unexpectedly large or unbounded response body, Traefik will allocate unlimited memory, potentially causing an out-of-memory (OOM) condition that crashes the process. This results in a denial of service for all routes served by the affected Traefik instance. This issue has been patched in versions 2.11.38 and 3.6.9.	4.4	More Details
CVE-2025-36105	IBM Planning Analytics Advanced Certified Containers 3.1.0 through 3.1.4 could allow a local privileged user to obtain sensitive information from environment variables.	4.4	More Details
CVE-2026-2420	The LotekMedia Popup Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the frontend of the site where the popup is displayed.	4.4	More Details
CVE-2026-28543	Race condition vulnerability in the maintenance and diagnostics module. Impact: Successful exploitation of this vulnerability may affect availability.	4.4	More Details
CVE-2026-1071	The Carta Online plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.13.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-30842	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.6.2, Wallos allows an authenticated user to delete avatar files uploaded by other users. The avatar deletion endpoint does not verify that the requested avatar belongs to the current user. As a result, any authenticated user who knows or can discover another user's uploaded avatar filename can delete that file. This issue has been patched in version 4.6.2.	4.3	More Details
CVE-2026-3702	A vulnerability was detected in SourceCodester Loan Management System 1.0. Affected by this issue is some unknown functionality of the file /index.php. Performing a manipulation of the argument page results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-3056	The Seraphinite Accelerator plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `seraph_accel_api` AJAX action with `fn=LogClear` in all versions up to, and including, 2.28.14. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the plugin's debug/operational logs.	4.3	More Details
CVE-2026-3058	The Seraphinite Accelerator plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.28.14 via the `seraph_accel_api` AJAX action with `fn=GetData`. This is due to the `OnAdminApi_GetData()` function not performing any capability checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive	4.3	More Details

	operational data including cache status, scheduled task information, and external database state.		
CVE-2026-3816	A security vulnerability has been detected in OWASP DefectDojo up to 2.55.4. This vulnerability affects the function input_zip.read of the file parser.py of the component SonarQubeParser/MSDefenderParser. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2.56.0 is able to resolve this issue. The identifier of the patch is e8f1e5131535b8fd80a7b1b3085d676295fdcd41. Upgrading the affected component is recommended.	4.3	More Details
CVE-2025-59544	Chamilo is a learning management system. Prior to version 1.11.34, the functionality for the user to update the category does not implement authorization checks for the "category_id" parameter which allows users to update the category of any user by replacing the "category_id" parameter. This issue has been patched in version 1.11.34.	4.3	More Details
CVE-2026-3770	A flaw has been found in SourceCodester Computer Laboratory Management System 1.0. This affects an unknown part. This manipulation causes cross-site request forgery. The attack is possible to be carried out remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2026-29773	Kubewarden is a policy engine for Kubernetes. Kubewarden cluster operators can grant permissions to users to deploy namespaced AdmissionPolicies and AdmissionPolicyGroups in their Namespaces. One of Kubewarden promises is that configured users can deploy namespaced policies in a safe manner, without privilege escalation. An attacker with privileged "AdmissionPolicy" create permissions (which isn't the default) could make use of 3 deprecated host-callback APIs: kubernetes/ingresses, kubernetes/namespaces, kubernetes/services. The attacker can craft a policy that exercises these deprecated API calls and would allow them read access to Ingresses, Namespaces, and Services resources respectively. This attack is read-only, there is no write capability and no access to Secrets, ConfigMaps, or other resource types beyond these three.	4.3	More Details
CVE-2026-1085	The True Ranker plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.9. This is due to missing nonce validation on the seolocalrank-signout action. This makes it possible for unauthenticated attackers to disconnect the administrator's True Ranker account via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-2488	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized message deletion due to a missing capability check on the pg_delete_msg() function in all versions up to, and including, 5.9.8.1. This is due to the function not verifying that the requesting user has permission to delete the targeted message. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary messages belonging to any user by sending a direct request with a valid message ID (mid parameter).	4.3	More Details
CVE-2026-1128	The WP eCommerce WordPress plugin through 3.15.1 does not have CSRF check in place when deleting coupons, which could allow attackers to make a logged in admin remove them via a CSRF attack	4.3	More Details
CVE-2026-2494	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.9.8.2. This is due to missing nonce validation on the membership request management page (approve and decline actions). This makes it possible for unauthenticated attackers to approve or deny group membership requests via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-2919	Malicious scripts could display attacker-controlled web content under spoofed domains in Focus for iOS by stalling a _self navigation to an invalid port and triggering an iframe redirect, causing the UI to display a trusted domain without user interaction. This vulnerability affects Focus for iOS < 148.2.	4.3	More Details
CVE-2026-3763	A vulnerability was found in code-projects Simple Flight Ticket Booking System 1.0. The affected element is an unknown function of the file showhistory.php. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-1981	The HUMN-1 AI Website Scanner & Human Certification by Winston AI plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the winston_disconnect() function in all versions up to, and including, 0.0.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's API connection settings via the 'winston_disconnect' AJAX action.	4.3	More Details
CVE-2026-27723	OpenProject is an open-source, web-based project management software. Prior to versions 17.0.5 and 17.1.2, an attacker can create wiki pages belonging to unpermitted projects through an improperly authenticated request. This issue has been patched in versions 17.0.5 and 17.1.2.	4.3	More Details

CVE-2026-3072	The Media Library Assistant plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the mla_update_compat_fields_action() function in all versions up to, and including, 3.33. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify taxonomy terms on arbitrary attachments.	4.3	More Details
CVE-2026-3610	A vulnerability was found in HSC Cybersecurity Mailinspector up to 5.3.2-3. Affected by this issue is some unknown functionality of the file /mailinspector/mliUserValidation.php of the component URL Handler. The manipulation of the argument error_description results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used. Upgrading to version 5.4.0 can resolve this issue. You should upgrade the affected component. The vendor was contacted early and responded very professional: "We have already implemented the fix and made a hotfix available to affected customers, ensuring mitigation while the official release 5.4.0 has not yet been published. This allows customers to address the issue immediately, outside the regular release cycle."	4.3	More Details
CVE-2026-1644	The WP Frontend Profile plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.8. This is due to missing nonce validation on the 'update_action' function. This makes it possible for unauthenticated attackers to approve or reject user account registrations via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-29049	melange allows users to build apk packages using declarative pipelines. In version 0.40.5 and prior, melange update-cache downloads URIs from build configs via io.Copy without any size limit or HTTP client timeout (pkg/renovate/cache/cache.go). An attacker-controlled URI in a melange config can cause unbounded disk writes, exhausting disk on the build runne. There is no known patch publicly available.	4.3	More Details
CVE-2026-1508	The Court Reservation WordPress plugin before 1.10.9 does not have CSRF check in place when deleting events, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.3	More Details
CVE-2026-28782	Craft is a content management system (CMS). Prior to 5.9.0-beta.1 and 4.17.0-beta.1, the "Duplicate" entry action does not properly verify if the user has permission to perform this action on the specific target elements. Even with only "View Entries" permission (where the "Duplicate" action is restricted in the UI), a user can bypass this restriction by sending a direct request. Furthermore, this vulnerability allows duplicating other users' entries by specifying their Entry IDs. Since Entry IDs are incremental, an attacker can trivially brute-force these IDs to duplicate and access restricted content across the system. This vulnerability is fixed in 5.9.0-beta.1 and 4.17.0-beta.1.	4.3	More Details
CVE-2026-28080	Missing Authorization vulnerability in Rank Math Rank Math SEO PRO allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Rank Math SEO PRO: from n/a through 3.0.95.	4.3	More Details
CVE-2026-1087	The Guardian News Feed plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to modify the plugin's settings, including the Guardian API key, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1086	The Font Pairing Preview For Landing Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to modify the plugin's font pairing settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-3812	A vulnerability was determined in itsourcecode Payroll Management System 1.0. Affected is an unknown function of the file /manage_employee_allowances.php. This manipulation of the argument ID causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-20069	A vulnerability in the VPN web services component of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct browser-based attacks against users of an affected device. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by persuading a user to visit a website that is designed to pass malicious HTTP requests to a device that is running Cisco Secure Firewall ASA Software or Cisco Secure FTD Software and has web services endpoints supporting VPN features enabled. A successful exploit could allow the attacker to reflect malicious input from the affected device to the browser that is in use and conduct browser-	4.3	More Details

	based attacks, including cross-site scripting (XSS) attacks. The attacker is not able to directly impact the affected device.		
CVE-2026-25972	An improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4 may allow a remote unauthenticated attacker to provide arbitrary data enabling a social engineering attack via spoofed URL parameters.	4.3	More Details
CVE-2026-20021	A vulnerability in the OSPF protocol of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, adjacent attacker to exhaust memory on an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improperly validating input by the OSPF protocol when parsing packets. An attacker could exploit this vulnerability by by sending crafted OSPF packets to an affected device. A successful exploit could allow the attacker to exhaust memory on the affected device, resulting in a DoS condition.	4.3	More Details
CVE-2026-1073	The Purchase Button For Affiliate Link plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing nonce validation on the settings page form handler in `inc/purchase-btn-options-page.php`. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2018-25168	Precurio Intranet Portal 2.0 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to create administrative user accounts by submitting crafted POST requests. Attackers can forge requests to the /public/admin/user/submitnew endpoint with user creation parameters to add new admin accounts without requiring CSRF tokens or user interaction.	4.3	More Details
CVE-2026-27661	A vulnerability has been identified in SINEC Security Monitor (All versions < V4.9.0). The affected application leaks confidential information in metadata, and files such as information on contributors and email address, on `SSM Server`.	4.3	More Details
CVE-2026-23812	A vulnerability has been identified where an attacker connecting to an access point as a standard wired or wireless client can impersonate a gateway by leveraging an address-based spoofing technique. Successful exploitation enables the redirection of data streams, allowing for the interception or modification of traffic intended for the legitimate network gateway via a Machine-in-the-Middle (MitM) position.	4.3	More Details
CVE-2026-23811	A vulnerability in the client isolation mechanism may allow an attacker to bypass Layer 2 (L2) communication restrictions between clients and redirect traffic at Layer 3 (L3). In addition to bypassing policy enforcement, successful exploitation - when combined with a port-stealing attack - may enable a bi-directional Machine-in-the-Middle (MitM) attack.	4.3	More Details
CVE-2026-23810	A vulnerability in the packet processing logic may allow an authenticated attacker to craft and transmit a malicious Wi-Fi frame that causes an Access Point (AP) to classify the frame as group-addressed traffic and re-encrypt it using the Group Temporal Key (GTK) associated with the victim's BSSID. Successful exploitation may enable GTK-independent traffic injection and, when combined with a port-stealing technique, allows an attacker to redirect intercepted traffic to facilitate machine-in-the-middle (MitM) attacks across BSSID boundaries.	4.3	More Details
CVE-2026-29190	Karapace is an open-source implementation of Kafka REST and Schema Registry. Prior to version 6.0.0, there is a Path Traversal vulnerability in the backup reader (backup/backends/v3/backend.py). If a malicious backup file is provided to Karapace, an attacker may exploit insufficient path validation to perform arbitrary file read on the system where Karapace is running. The issue affects deployments that use the backup/restore functionality and process backups from untrusted sources. The impact depends on the file system permissions of the Karapace process. This issue has been patched in version 6.0.0.	4.1	More Details
CVE-2025-55717	A cleartext storage of sensitive information vulnerability [CWE-312] vulnerability in Fortinet FortiMail 7.6.0 through 7.6.2, FortiMail 7.4.0 through 7.4.4, FortiMail 7.2.0 through 7.2.7, FortiMail 7.0.0 through 7.0.8, FortiRecorder 7.2.0 through 7.2.3, FortiRecorder 7.0 all versions, FortiRecorder 6.4 all versions, FortiVoice 7.2.0, FortiVoice 7.0.0 through 7.0.6 may allow an authenticated malicious administrator to obtain user's secrets via CLI commands. Practical exploitability is limited by conditions out of the control of the attacker: An admin must log in to the targeted device.	4.0	More Details
CVE-2026-28540	Out-of-bounds character read vulnerability in Bluetooth. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-16 and 6.9.13-41, a heap-use-after-free vulnerability exists in the MSL encoder,		More

2026-28688	where a cloned image is destroyed twice. The MSL coder does not support writing MSL so the write capability has been removed. This vulnerability is fixed in 7.1.2-16 and 6.9.13-41.	4.0	Details
CVE-2026-29795	stellar-xdr is a library and CLI containing types and functionality for working with Stellar XDR. Prior to version 25.0.1, StringM::from_str does not validate that the input length is within the declared maximum (MAX). Calling StringM::<N>::from_str(s) where s is longer than N bytes succeeds and returns an Ok value instead of Err(Error::LengthExceedsMax), producing a StringM that violates its length invariant. This affects any code that constructs StringM values from string input using FromStr (including str::parse), and relies on the type's maximum length constraint being enforced. An oversized StringM could propagate through serialization, validation, or other logic that assumes the invariant holds. This issue has been patched in version 25.0.1.	4.0	More Details
CVE-2026-28541	Permission control vulnerability in the cellular_data module. Impact: Successful exploitation of this vulnerability may affect availability.	4.0	More Details
CVE-2026-28550	Race condition vulnerability in the security control module. Impact: Successful exploitation of this vulnerability may affect availability.	4.0	More Details
CVE-2026-22629	An improper restriction of excessive authentication attempts vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4 all versions, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer 6.4 all versions, FortiAnalyzer Cloud 7.6.2, FortiAnalyzer Cloud 7.4.1 through 7.4.7, FortiAnalyzer Cloud 7.2.1 through 7.2.10, FortiAnalyzer Cloud 7.0.1 through 7.0.14, FortiAnalyzer Cloud 6.4 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4 all versions, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager 6.4 all versions, FortiManager Cloud 7.6.2 through 7.6.3, FortiManager Cloud 7.4.1 through 7.4.7, FortiManager Cloud 7.2.1 through 7.2.10, FortiManager Cloud 7.0.1 through 7.0.14, FortiManager Cloud 6.4 all versions may allow an attacker to bypass bruteforce protections via exploitation of race conditions. The latter raises the complexity of practical exploitation.	3.7	More Details
CVE-2026-3706	A vulnerability was determined in mkj Dropbear up to 2025.89. Impacted is the function unpackneg of the file src/curve25519.c of the component S Range Check. This manipulation causes improper verification of cryptographic signature. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is considered difficult. The exploit has been publicly disclosed and may be utilized. Patch name: fdec3c90a15447bd538641d85e5a3e3ac981011d. To fix this issue, it is recommended to deploy a patch.	3.7	More Details
CVE-2026-30848	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.8 and 9.5.0-alpha.8, the PagesRouter static file serving route is vulnerable to a path traversal attack that allows unauthenticated reading of files outside the configured pagesPath directory. The boundary check uses a string prefix comparison without enforcing a directory separator boundary. An attacker can use path traversal sequences to access files in sibling directories whose names share the same prefix as the pages directory (e.g. pages-secret starts with pages). This issue has been patched in versions 8.6.8 and 9.5.0-alpha.8.	3.7	More Details
CVE-2025-15603	A security vulnerability has been detected in open-webui up to 0.6.16. Affected is an unknown function of the file backend/start_windows.bat of the component JWT Key Handler. Such manipulation of the argument WEBUI_SECRET_KEY leads to insufficiently random values. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitability is told to be difficult. The exploit has been disclosed publicly and may be used.	3.7	More Details
CVE-2025-11143	The Jetty URI parser has some key differences to other common parsers when evaluating invalid or unusual URIs. Differential parsing of URIs in systems using multiple components may result in security by-pass. For example a component that enforces a black list may interpret the URIs differently from one that generates a response. At the very least, differential parsing may divulge implementation details.	3.7	More Details
CVE-2026-3742	A vulnerability was detected in YiFang CMS 2.0.5. The impacted element is the function update of the file app/db/admin/D_singlePage.php. Performing a manipulation of the argument Title results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-3766	A security flaw has been discovered in SourceCodester Web-based Pharmacy Product Management System 1.0. This impacts an unknown function of the file edit-profile.php. Performing a manipulation of the argument fullname results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	3.5	More Details

CVE-2026-24310	Due to missing authorization check in SAP NetWeaver Application Server for ABAP, an authenticated attacker could execute specific ABAP function module and read the sensitive information from database catalog of the ABAP system. This vulnerability has low impact on the application's confidentiality with no effect on the integrity and availability.	3.5	More Details
CVE-2026-3819	A vulnerability has been found in SourceCodester Resort Reservation System 1.0. The affected element is an unknown function of the file /?page=manage_reservation of the component Reservation Management Module. Such manipulation of the argument ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-3741	A security vulnerability has been detected in YiFang CMS 2.0.5. The affected element is the function update of the file app/db/admin/D_friendLink.php. Such manipulation of the argument linkName leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-3720	A security flaw has been discovered in 1024-lab/lab1024 SmartAdmin up to 3.29. Impacted is an unknown function of the file smart-admin-web-javascript/src/views/business/oa/notice/components/notice-form-drawer.vue of the component Notice Module. The manipulation results in cross site scripting. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-3721	A weakness has been identified in 1024-lab/lab1024 SmartAdmin up to 3.29. The affected element is an unknown function of the file sa-base/src/main/java/net/lab1024/sa/base/module/support/helpdoc/domain/form/HelpDocAddForm.java of the component Help Documentation Module. This manipulation causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-3743	A flaw has been found in YiFang CMS 2.0.5. This affects the function update of the file app/db/admin/D_singlePageGroup.php. Executing a manipulation of the argument Name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-21422	Dell PowerScale OneFS, versions 9.10.0.0 through 9.10.1.5 and versions 9.11.0.0 through 9.12.0.1, contains an external control of system or configuration setting vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to protection mechanism bypass.	3.4	More Details
CVE-2025-68467	Dark Reader is an accessibility browser extension that makes web pages colors dark. The dynamic dark mode feature of the extension works by analyzing the colors of web pages found in CSS style sheet files. In order to analyze cross-origin style sheets (stored on websites different from the original web page), Dark Reader requests such files via a background worker, ensuring the request is performed with no credentials and that the content type of the response is a CSS file. Prior to Dark Reader 4.9.117, this style content was assigned to an HTML Style Element in order to parse and loop through style declarations, and also stored in page's Session Storage for performance gains. This could allow a website author to request a style sheet from a locally running web server, for example by having a link pointing to `http[:]//localhost[:]8080/style[.]css`. The brute force of the host name, port and file name would be unlikely due to performance impact, that would cause the browser tab to hang shortly, but it could be possible to request a style sheet if the full URL was known in advance. As per December 18, 2025 there is no known exploit of the issue. The problem has been fixed in version 4.9.117 on December 3, 2025. The style sheets are now parsed using modern Constructed Style Sheets API and the contents of cross-origin style sheets is no longer stored in page's Session Storage. Version 4.9.118 (December 8, 2025) restricts cross-origin requests to localhost aliases, IP addresses, hosts with ports and non-HTTPS resources. The absolute majority of users have received an update 4.1.117 or 4.9.118 automatically within a week. However users must ensure their automatic updates are not blocked and they are using the latest version of the extension by going to chrome://extensions or about:addons pages in browser settings. Users utilizing manual builds must upgrade to version 4.9.118 and above. Developers using `darkreader` NPM package for their own websites are likely not affected, but must ensure the function passed to `setFetchMethod()` for performing cross-origin requests works within the intended scope. Developers using custom forks of earlier versions of Dark Reader to build other extensions or integrating into their apps or browsers must ensure they perform cross-origin requests safely and the responses are not accessible outside of the app or extension.	3.4	More Details
CVE-2026-22760	Dell Device Management Agent (DDMA), versions prior to 26.02, contain an Improper Check for Unusual or Exceptional Conditions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of Service.	3.3	More Details

CVE-2026-3663	A vulnerability was found in xlnt-community xlnt up to 1.6.1. This issue affects the function xlnt::detail::compound_document_istreambuf::xsgetn of the file source/detail/cryptography/compound_document.cpp of the component XLSX File Parser. Performing a manipulation results in out-of-bounds read. The attack is only possible with local access. The exploit has been made public and could be used. The patch is named 147. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2026-3606	A vulnerability has been found in Ettercap 0.8.4-Garofalo. Affected by this vulnerability is the function add_data_segment of the file src/ettercap/utils/etterfilter/ef_output.c of the component etterfilter. The manipulation leads to out-of-bounds read. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-21791	HCL Sametime for Android is impacted by a sensitive information disclosure. Hostnames information is written in application logs and certain URL	3.3	More Details
CVE-2025-66319	Permission control vulnerability in the resource scheduling module. Impact: Successful exploitation of this vulnerability may affect service integrity.	3.3	More Details
CVE-2026-3665	A vulnerability was identified in xlnt-community xlnt up to 1.6.1. The affected element is the function xlnt::detail::xlsx_consumer::read_office_document of the file source/detail/serialization/xlsx_consumer.cpp of the component XLSX File Parser. The manipulation leads to null pointer dereference. The attack must be carried out locally. The exploit is publicly available and might be used.	3.3	More Details
CVE-2026-21786	HCL Sametime for iOS is impacted by a sensitive information disclosure. Hostnames information is written in application logs and certain URLs.	3.3	More Details
CVE-2026-3664	A vulnerability was determined in xlnt-community xlnt up to 1.6.1. Impacted is the function xlnt::detail::compound_document::read_directory of the file source/detail/cryptography/compound_document.cpp of the component Encrypted XLSX File Parser. Executing a manipulation can lead to out-of-bounds read. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized. This patch is called 147. Applying a patch is advised to resolve this issue.	3.3	More Details
CVE-2026-3671	A flaw has been found in Freedom Factory dGEN1 up to 20260221. Affected by this vulnerability is the function TokenBalanceContentProvider of the component org.ethereumphone.walletmanager.testing123. Executing a manipulation can lead to improper authorization. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2026-3668	A weakness has been identified in Freedom Factory dGEN1 up to 20260221. This affects the function AndroidEthereum of the component org.ethosmobile.webpwaemul. This manipulation causes improper access controls. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is reported as difficult. 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.	3.1	More Details
CVE-2026-2671	A vulnerability was detected in Mendi Neurofeedback Headset V4. Affected by this vulnerability is an unknown functionality of the component Bluetooth Low Energy Handler. Performing a manipulation results in cleartext transmission of sensitive information. The attack can only be performed from the local network. The attack's complexity is rated as high. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-0121	In VPU, there is a possible use-after-free read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2.9	More Details
CVE-2026-29185	Backstage is an open framework for building developer portals. Prior to version 1.20.1, a vulnerability in the SCM URL parsing used by Backstage integrations allowed path traversal sequences in encoded form to be included in file paths. When these URLs were processed by integration functions that construct API URLs, the traversal segments could redirect requests to unintended SCM provider API endpoints using the configured server-side integration credentials. This issue has been patched in version 1.20.1.	2.7	More Details
CVE-	A NULL Pointer Dereference vulnerability [CWE-476] vulnerability in Fortinet FortiWeb 8.0.0 through		

2026-24641	8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow an authenticated attacker to crash the HTTP daemon via crafted HTTP requests.	2.7	More Details
CVE-2025-27769	A vulnerability has been identified in Heliox Flex 180 kW EV Charging Station (All versions < F4.11.1), Heliox Mobile DC 40 kW EV Charging Station (All versions < L4.10.1). Affected devices contain improper access control that could allow an attacker to reach unauthorized services via the charging cable.	2.6	More Details
CVE-2026-27139	On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.	2.5	More Details
CVE-2026-3716	A vulnerability was determined in Wavlink WL-WN579X3-C 231124. This vulnerability affects the function sub_401AD4 of the file /cgi-bin/adm.cgi. Executing a manipulation of the argument Hostname can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 20260226 is able to resolve this issue. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2.4	More Details
CVE-2026-29110	Cryptomator encrypts data being stored on cloud infrastructure. Prior to version 1.19.0, in non-debug mode Cryptomator might leak cleartext paths into the log file. This can reveal meta information about the files stored inside a vault at a time, where the actual vault is closed. Not every cleartext path is logged. Only if a filesystem request fails for some reason (e.g. damaged encrypted file, not existing file), a log message is created. This issue has been patched in version 1.19.0.	2.2	More Details
CVE-2026-29184	Backstage is an open framework for building developer portals. Prior to version 3.1.4, a malicious scaffolder template can bypass the log redaction mechanism to exfiltrate secrets provided run through task event logs. This issue has been patched in version 3.1.4.	2.0	More Details
CVE-2026-30825	hoppscotch is an open source API development ecosystem. Prior to version 2026.2.1, the DELETE /v1/access-tokens/revoke endpoint allows any authenticated user to delete any other user's PAT by providing its ID, with no ownership verification. This issue has been patched in version 2026.2.1.	0.0	More Details
CVE-2026-30969	Coral Server is open collaboration infrastructure that enables communication, coordination, trust and payments for The Internet of Agents. Prior to 1.1.0, Coral Server did not enforce strong authentication between agents and the server within an active session. This could allow an attacker who obtained or predicted a session identifier to impersonate an agent or join an existing session. This vulnerability is fixed in 1.1.0.	N/A	More Details
CVE-2025-20073	Improper buffer restrictions in the UEFI DXE module for some Intel(R) Reference Platforms within UEFI may allow an information disclosure. System software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2025-71238	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix bsg_done() causing double free Kernel panic observed on system, [5353358.825191] BUG: unable to handle page fault for address: ff5f5e897b024000 [5353358.825194] #PF: supervisor write access in kernel mode [5353358.825195] #PF: error_code(0x0002) - not-present page [5353358.825196] PGD 100006067 P4D 0 [5353358.825198] Oops: 0002 [#1] PREEMPT SMP NOPTI [5353358.825200] CPU: 5 PID: 2132085 Comm: qlafwupdate.sub Kdump: loaded Tainted: G W L ------- --- 5.14.0-503.34.1.el9_5.x86_64 #1 [5353358.825203] Hardware name: HPE ProLiant DL360 Gen11/ProLiant DL360 Gen11, BIOS 2.44 01/17/2025 [5353358.825204] RIP: 0010:memcpy_erms+0x6/0x10 [5353358.825211] RSP: 0018:ff591da8f4f6b710 EFLAGS: 00010246 [5353358.825212] RAX: ff5f5e897b024000 RBX: 0000000000007090 RCX: 0000000000001000 [5353358.825213] RDX: 0000000000001000 RSI: ff591da8f4fed090 RDI: ff5f5e897b024000 [5353358.825214] RBP: 0000000000010000 R08: ff5f5e897b024000 R09: 0000000000000000 [5353358.825215] R10: ff46cf8c40517000 R11: 0000000000000001 R12: 0000000000008090 [5353358.825216] R13: ff591da8f4f6b720 R14: 0000000000001000 R15: 0000000000000000 [5353358.825218] FS: 00007f1e88d47740(0000) GS:ff46cf935f940000(0000) knlGS:0000000000000000 [5353358.825219] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [5353358.825220] CR2: ff5f5e897b024000 CR3: 0000000231532004 CR4: 0000000000771ef0 [5353358.825221] PKRU: 55555554 [5353358.825222] Call Trace: [5353358.825223] <TASK> [5353358.825224] ? show_trace_log_lvl+0x1c4/0x2df [5353358.825229] ? show_trace_log_lvl+0x1c4/0x2df [5353358.825232] ? sg_copy_buffer+0xc8/0x110 [5353358.825236] ? __die_body.cold+0x8/0xd	N/A	More Details

	[5353358.825238] ? page_fault_oops+0x134/0x170 [5353358.825242] ? kernelmode_fixup_or_oops+0x84/0x110 [5353358.825244] ? exc_page_fault+0xa8/0x150 [5353358.825247] ? asm_exc_page_fault+0x22/0x30 [5353358.825252] ? memcpy_erms+0x6/0x10 [5353358.825253] sg_copy_buffer+0xc8/0x110 [5353358.825259] qla2x00_process_vendor_specific+0x652/0x1320 [qla2xxx] [5353358.825317] qla24xx_bsg_request+0x1b2/0x2d0 [qla2xxx] Most routines in qla_bsg.c call bsg_done() only for success cases. However a few invoke it for failure case as well leading to a double free. Validate before calling bsg_done().		
CVE-2026-30959	OneUptime is a solution for monitoring and managing online services. The resend-verification-code endpoint allows any authenticated user to trigger a verification code resend for any UserWhatsApp record by ID. Ownership is not validated (unlike the verify endpoint). This affects the UserWhatsAppAPI.ts endpoint and the UserWhatsAppService.ts service.	N/A	More Details
CVE-2026-28725	Sensitive information disclosure due to improper configuration of a headless browser. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-0124	There is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-30948	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.4 and 8.6.17, a stored cross-site scripting (XSS) vulnerability allows any authenticated user to upload an SVG file containing JavaScript. The file is served inline with Content-Type: image/svg+xml and without protective headers, causing the browser to execute embedded scripts in the Parse Server origin. This can be exploited to steal session tokens from localStorage and achieve account takeover. The default fileExtensions option blocks HTML file extensions but does not block SVG, which is a well-known XSS vector. All Parse Server deployments where file upload is enabled for authenticated users (the default) are affected. This vulnerability is fixed in 9.5.2-alpha.4 and 8.6.17.	N/A	More Details
CVE-2026-30949	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.5 and 8.6.18, the Keycloak authentication adapter does not validate the azp (authorized party) claim of Keycloak access tokens against the configured client-id. A valid access token issued by the same Keycloak realm for a different client application can be used to authenticate as any user on the Parse Server that uses the Keycloak adapter. This enables cross-application account takeover in multi-client Keycloak realms. All Parse Server deployments that use the Keycloak authentication adapter with a Keycloak realm that has multiple client applications are affected. This vulnerability is fixed in 9.5.2-alpha.5 and 8.6.18.	N/A	More Details
CVE-2026-23231	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix use-after-free in nf_tables_addchain() nf_tables_addchain() publishes the chain to table->chains via list_add_tail_rcu() (in nft_chain_add()) before registering hooks. If nf_tables_register_hook() then fails, the error path calls nft_chain_del() (list_del_rcu()) followed by nf_tables_chain_destroy() with no RCU grace period in between. This creates two use-after-free conditions: 1) Control-plane: nf_tables_dump_chains() traverses table->chains under rcu_read_lock(). A concurrent dump can still be walking the chain when the error path frees it. 2) Packet path: for NFPROTO_INET, nf_register_net_hook() briefly installs the IPv4 hook before IPv6 registration fails. Packets entering nft_do_chain() via the transient IPv4 hook can still be dereferencing chain->blob_gen_X when the error path frees the chain. Add synchronize_rcu() between nft_chain_del() and the chain destroy so that all RCU readers -- both dump threads and in-flight packet evaluation -- have finished before the chain is freed.	N/A	More Details
CVE-2026-30960	rssn is a scientific computing library for Rust, combining a high-performance symbolic computation engine with numerical methods support and physics simulations functionalities. The vulnerability exists in the JIT (Just-In-Time) compilation engine, which is fully exposed via the CFFI (Foreign Function Interface). Due to Improper Input Validation and External Control of Code Generation, an attacker can supply malicious parameters or instruction sequences through the CFFI layer. Since the library often operates with elevated privileges or within high-performance computing contexts, this allows for Arbitrary Code Execution (ACE) at the privilege level of the host process.	N/A	More Details
CVE-2025-20105	Improper input validation in some UEFI firmware SMM module for the Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (high) impacts.	N/A	More Details

CVE-2025-20096	Improper input validation in the UEFI firmware for some Intel Reference Platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (none), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (high) and availability (high) impacts.	N/A	More Details
CVE-2026-30968	Coral Server is open collaboration infrastructure that enables communication, coordination, trust and payments for The Internet of Agents. Prior to 1.1.0, the SSE endpoint (/sse/v1/...) in Coral Server did not strongly validate that a connecting agent was a legitimate participant in the session. This could theoretically allow unauthorized message injection or observation. This vulnerability is fixed in 1.1.0.	N/A	More Details
CVE-2026-30952	liquidjs is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.0, the layout, render, and include tags allow arbitrary file access via absolute paths (either as string literals or through Liquid variables, the latter require dynamicPartials: true, which is the default). This poses a security risk when malicious users are allowed to control the template content or specify the filepath to be included as a Liquid variable. This vulnerability is fixed in 10.25.0.	N/A	More Details
CVE-2026-24732	Files or Directories Accessible to External Parties, Incorrect Permission Assignment for Critical Resource vulnerability in Hallo Welt! GmbH BlueSpice (Extension:NSFileRepo modules) allows Accessing Functionality Not Properly Constrained by ACLs, Bypassing Electronic Locks and Access Controls.This issue affects BlueSpice: from 5.1 through 5.1.3, from 5.2 through 5.2.0. HINT: Versions provided apply to BlueSpice MediaWiki releases. For Extension:NSFileRepo the affected versions are 3.0 < 3.0.5	N/A	More Details
CVE-2026-30970	Coral Server is open collaboration infrastructure that enables communication, coordination, trust and payments for The Internet of Agents. Prior to 1.1.0, Coral Server allowed the creation of agent sessions through the /api/v1/sessions endpoint without strong authentication. This endpoint performs resource-intensive initialization operations including container spawning and memory context creation. An attacker capable of accessing the endpoint could create sessions or consume system resources without proper authorization. This vulnerability is fixed in 1.1.0.	N/A	More Details
CVE-2025-22444	Exposure of resource to wrong sphere in the UEFI PdaSmm module for some Intel(R) reference platforms may allow an information disclosure. System software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2026-28713	Default credentials set for local privileged user in Virtual Appliance. The following products are affected: Acronis Cyber Protect Cloud Agent (VMware) before build 36943, Acronis Cyber Protect 17 (VMware) before build 41186.	N/A	More Details
CVE-2025-22850	Time-of-check time-of-use race condition in the UEFI PdaSmm module for some Intel(R) reference platforms may allow an information disclosure. System software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2026-30947	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.3 and 8.6.16, class-level permissions (CLP) are not enforced for LiveQuery subscriptions. An unauthenticated or unauthorized client can subscribe to any LiveQuery-enabled class and receive real-time events for all objects, regardless of CLP restrictions. All Parse Server deployments that use LiveQuery with class-level permissions are affected. Data intended to be restricted by CLP is leaked to unauthorized subscribers in real time. This vulnerability is fixed in 9.5.2-alpha.3 and 8.6.16.	N/A	More Details
CVE-2026-30977	RenderBlocking is a MediaWiki extension that allows interface administrators to specify render-blocking CSS and JavaScript. Prior to 0.1.1, there is Stored XSS in renderblocking-css with Inline Assets mode. $wgRenderBlockingInlineAssets = true and editsitecss user rights are required. This vulnerability is fixed in 0.1.1.	N/A	More Details
CVE-2026-28719	Unauthorized resource manipulation due to improper authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details

CVE-2026-31819	Sylius is an Open Source eCommerce Framework on Symfony. CurrencySwitchController::switchAction(), ImpersonateUserController::impersonateAction() and StorageBasedLocaleSwitcher::handle() use the HTTP Referer header directly when redirecting. The attack requires the victim to click a legitimate application link placed on an attacker-controlled page. The browser automatically sends the attacker's site as the Referer, and the application redirects back to it. This can be used for phishing or credential theft, as the redirect originates from a trusted domain. The severity varies by endpoint; public endpoints require no authentication and are trivially exploitable, while admin-only endpoints require an authenticated session but remain vulnerable if an admin follows a link from an external source such as email or chat. The issue is fixed in versions: 1.9.12, 1.10.16, 1.11.17, 1.12.23, 1.13.15, 1.14.18, 2.0.16, 2.1.12, 2.2.3 and above.	N/A	More Details
CVE-2026-28776	International Datacasting Corporation (IDC) SFX Series SuperFlex SatelliteReceiver contains hardcoded credentials for the \`monitor\` account. A remote unauthenticated attacker can use these trivial, undocumented credentials to access the system via SSH. While initially dropped into a restricted shell, the attacker can trivially break out to achieve standard shell functionality.	N/A	More Details
CVE-2025-20068	Improper input validation in the UEFI ImcErrorHandler module for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2026-29176	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 5.5.3, A stored XSS vulnerability exists in the Commerce Settings - Inventory Locations page. The Name field is rendered without proper HTML escaping, allowing an attacker to execute arbitrary JavaScript. This XSS triggers when an administrator (or user with product editing permissions) creates or edits a variant product. This vulnerability is fixed in 5.5.3.	N/A	More Details
CVE-2026-0111	In ns_GetUserData of ns_SmscbUtilities.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-29175	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 5.5.3, Stored XSS vulnerabilities exist in the Commerce Inventory page. The Product Title, Variant Title, and Variant SKU fields are rendered without proper HTML escaping, allowing an attacker to execute arbitrary JavaScript when any user (including administrators) views the inventory management page. This vulnerability is fixed in 5.5.3.	N/A	More Details
CVE-2026-29174	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 5.5.3, Craft Commerce is vulnerable to SQL Injection in the inventory levels table data endpoint. The sort[0][direction] and sort[0][sortField] parameters are concatenated directly into an addOrderBy() clause without any validation or sanitization. An authenticated attacker with access to the Commerce Inventory section can inject arbitrary SQL queries, potentially leading to a full database compromise. This vulnerability is fixed in 5.5.3.	N/A	More Details
CVE-2026-29173	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 4.10.2 and 5.5.3, a stored XSS vulnerability exists when a user tries to update the Order Status from the Commerce Orders Table. The Order Status Name is rendered without proper escaping, allowing script execution to occur. This vulnerability is fixed in 4.10.2 and 5.5.3.	N/A	More Details
CVE-2026-29172	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 4.10.2 and 5.5.3, Craft Commerce is vulnerable to SQL Injection in the purchasables table endpoint. The sort parameter is split by | and the first part (column name) is passed directly as an array key to orderBy() without whitelist validation. Yii2's query builder does NOT escape array keys, allowing an authenticated attacker to inject arbitrary SQL into the ORDER BY clause. This vulnerability is fixed in 4.10.2 and 5.5.3.	N/A	More Details
CVE-2026-29113	Craft is a content management system (CMS). Prior to 4.17.4 and 5.9.7, Craft CMS has a CSRF issue in the preview token endpoint at /actions/preview/create-token. The endpoint accepts an attacker-supplied previewToken. Because the action does not require POST and does not enforce a CSRF token, an attacker can force a logged-in victim editor to mint a preview token chosen by the attacker. That token can then be used by the attacker (without authentication) to access previewed/unpublished content tied to the victim’s authorized preview scope. This vulnerability is fixed in 4.17.4 and 5.9.7.	N/A	More Details
CVE-2026-0112	In vpu_open_inst of vpu_ioctl.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details

CVE-2026-0113	In ns_GetUserData of ns_SmscbUtilities.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-0114	In Modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-29120	The /root/anaconda-ks.cfg installation configuration file in International Datacasting Corporation (IDC) SFX Series(SFX2100) SuperFlex Satellite Receiver insecurely stores the hardcoded root password hash. The password itself is highly insecure and susceptible to offline dictionary attacks using the rockyou.txt wordlist. Because direct root SSH login is disabled, an attacker must first obtain low-privileged access to the system (e.g., via other vulnerabilities) to be able to log in as the root user. The password is hardcoded and so allows for an actor with local access on effected versions to escalate to root	N/A	More Details
CVE-2026-28807	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in gleam-wisp wisp allows arbitrary file read via percent-encoded path traversal. The wisp.serve_static function is vulnerable to path traversal because sanitization runs before percent-decoding. The encoded sequence %2e%2e passes through string.replace unchanged, then uri.percent_decode converts it to .., which the OS resolves as directory traversal when the file is read. An unauthenticated attacker can read any file readable by the application process in a single HTTP request, including application source code, configuration files, secrets, and system files. This issue affects wisp: from 2.1.1 before 2.2.1.	N/A	More Details
CVE-2026-28806	Improper Authorization vulnerability in nerves-hub nerves_hub_web allows cross-organization device control via device bulk actions and device update API. Missing authorization checks in the device bulk actions and device update API endpoints allow authenticated users to target devices belonging to other organizations and perform actions outside of their privilege level. An attacker can select devices outside of their organization by manipulating device identifiers and perform management actions on them, such as moving them to products they control. This may allow attackers to interfere with firmware updates, access device functionality exposed by the platform, or disrupt device connectivity. In environments where additional features such as remote console access are enabled, this could lead to full compromise of affected devices. This issue affects nerves_hub_web: from 1.0.0 before 2.4.0.	N/A	More Details
CVE-2026-23868	Giflib contains a double-free vulnerability that is the result of a shallow copy in GifMakeSavedImage and incorrect error handling. The conditions needed to trigger this vulnerability are difficult but may be possible.	N/A	More Details
CVE-2026-27446	Missing Authentication for Critical Function (CWE-306) vulnerability in Apache Artemis, Apache ActiveMQ Artemis. An unauthenticated remote attacker can use the Core protocol to force a target broker to establish an outbound Core federation connection to an attacker-controlled rogue broker. This could potentially result in message injection into any queue and/or message exfiltration from any queue via the rogue broker. This impacts environments that allow both: - incoming Core protocol connections from untrusted sources to the broker - outgoing Core protocol connections from the broker to untrusted targets This issue affects: - Apache Artemis from 2.50.0 through 2.51.0 - Apache ActiveMQ Artemis from 2.11.0 through 2.44.0. Users are recommended to upgrade to Apache Artemis version 2.52.0, which fixes the issue. The issue can be mitigated by either of the following: - Remove Core protocol support from any acceptor receiving connections from untrusted sources. Incoming Core protocol connections are supported by default via the "artemis" acceptor listening on port 61616. See the "protocols" URL parameter configured for the acceptor. An acceptor URL without this parameter supports all protocols by default, including Core. - Use two-way SSL (i.e. certificate-based authentication) in order to force every client to present the proper SSL certificate when establishing a connection before any message protocol handshake is attempted. This will prevent unauthenticated exploitation of this vulnerability.	N/A	More Details
CVE-2026-0115	In Trusted Execution Environment, there is a possible key leak due to side channel information disclosure. This could lead to physical information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	N/A	More Details
CVE-2025-70129	If the anti spam-captcha functionality in PluXml versions 5.8.22 and earlier is enabled, a captcha challenge is generated with a format that can be automatically recognized for articles, such that an automated script is able to solve this anti-spam mechanism trivially and publish spam comments. The details of captcha challenge are exposed within document body of articles with comments & anti spam-captcha functionalities enabled, including "capcha-letter", "capcha-word" and "capcha-token" which can be used to construct a valid post request to publish a comment. As such, attackers can flood articles with automated spam comments, especially if there are no other web defenses available.	N/A	More Details
CVE-	Craft Commerce is an ecommerce platform for Craft CMS. Prior to 4.10.2 and 5.5.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Craft Commerce Order details. Malicious JavaScript can be		

2026-29177	injected via the Shipping Method Name, Order Reference, or Site Name. When a user opens the order details slideout via a double-click on the order index page, the injected payload executes. This vulnerability is fixed in 4.10.2 and 5.5.3.	N/A	More Details
CVE-2026-29792	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. From 5.0.0 to before 5.0.42, an unauthenticated attacker can send a crafted GET request directly to /oauth/:provider/callback with a forged profile in the query string. The OAuth service's authentication payload has a fallback chain that reaches params.query (the raw request query) when Grant's session/state responses are empty. Since the attacker never initiated an OAuth authorize flow, Grant has no session to work with and produces no response, so the fallback fires. The forged profile then drives entity lookup and JWT minting. The attacker gets a valid access token for an existing user without ever contacting the OAuth provider. This vulnerability is fixed in 5.0.42.	N/A	More Details
CVE-2026-29793	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. From 5.0.0 to before 5.0.42, Socket.IO clients can send arbitrary JavaScript objects as the id argument to any service method (get, patch, update, remove). The transport layer performs no type checking on this argument. When the service uses the MongoDB adapter, these objects pass through getObjectId() and land directly in the MongoDB query as operators. Sending {$ne: null} as the id matches every document in the collection. This vulnerability is fixed in 5.0.42.	N/A	More Details
CVE-2025-70798	Tenda i24V3.0si V3.0.0.5 Firmware V3.0.0.5 was discovered to contain a hardcoded password vulnerability in /etc_ro/shadow, which allows attackers to log in as root.	N/A	More Details
CVE-2026-0108	The register protection of the PowerVR GPU is incorrectly configured. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-23232	In the Linux kernel, the following vulnerability has been resolved: Revert "f2fs: block cache/dio write during f2fs_enable_checkpoint()" This reverts commit 196c81fdd438f7ac429d5639090a9816abb9760a. Original patch may cause below deadlock, revert it. write remount - write_begin - lock_page --- lock A - prepare_write_begin - f2fs_map_lock - f2fs_enable_checkpoint - down_write(cp_enable_rwsem) --- lock B - sync_inode_sb - writepages - lock_page --- lock A - down_read(cp_enable_rwsem) --- lock A	N/A	More Details
CVE-2026-0107	In gmc_ddr_handle_mba_mr_req of gmc_mba_ddr.c, there is a possible escalation of privileges due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-31821	Sylius is an Open Source eCommerce Framework on Symfony. The POST /api/v2/shop/orders/{tokenValue}/items endpoint does not verify cart ownership. An unauthenticated attacker can add items to other registered customers' carts by knowing the cart tokenValue. An attacker who obtains a cart tokenValue can add arbitrary items to another customer's cart. The endpoint returns the full cart representation in the response (HTTP 201). The issue is fixed in versions: 2.0.16, 2.1.12, 2.2.3 and above.	N/A	More Details
CVE-2026-31822	Sylius is an Open Source eCommerce Framework on Symfony. A cross-site scripting (XSS) vulnerability exists in the shop checkout login form handled by the ApiLoginController Stimulus controller. When a login attempt fails, AuthenticationFailureHandler returns a JSON response whose message field is rendered into the DOM using innerHTML, allowing any HTML or JavaScript in that value to be parsed and executed by the browser. The issue is fixed in versions: 2.0.16, 2.1.12, 2.2.3 and above.	N/A	More Details
CVE-2026-0109	In dhd_tcpdata_info_get of dhd_ip.c, there is a possible Denial of Service due to a precondition check failure. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-70802	Tenda G1V3.1si V16.01.7.8 Firmware V16.01.7.8 was discovered to contain a hardcoded password vulnerability in /etc_ro/shadow, which allows attackers to log in as root.	N/A	More Details
CVE-2026-0110	In MM_DATA_IND of cn_NrSmMsgHdlrFromMM.cpp, there is a possible EoP due to memory corruption. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-	An improper neutralization of input vulnerability was identified in GitHub Enterprise Server that allowed DOM-based cross-site scripting via task list content. The task list content extraction logic did not properly re-encode browser-decoded text nodes before rendering, allowing user-supplied HTML to be injected into the page. An authenticated attacker could craft malicious task list items in issues or	N/A	More Details

2266	pull requests to execute arbitrary scripts in the context of another user's browser session. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.20 and was fixed in versions 3.18.6 and 3.19.3. This vulnerability was reported via the GitHub Bug Bounty program.		
CVE-2026-28777	International Datacasting Corporation (IDC) SFX2100 Satellite Receiver, trivial password for the `user` (usr) account. A remote unauthenticated attacker can exploit this to gain unauthorized SSH access to the system, while intially dropped into a restricted shell, an attacker can trivially spawn a complete pty to gain an appropriately interactive shell.	N/A	More Details
CVE-2026-28723	Unauthorized report deletion due to insufficient access control. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-28778	International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver contains undocumented, hardcoded/insecure credentials for the `xd` user account. A remote unauthenticated attacker can log in via FTP using these credentials. Because the `xd` user has write permissions to their home directory where root-executed binaries and symlinks (such as those invoked by `xdstartstop`) are stored, the attacker can overwrite these files or manipulate symlinks to achieve arbitrary code execution as the root user.	N/A	More Details
CVE-2025-36920	In hyp_alloc of arch/arm64/kvm/hyp/nvhe/alloc.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-3582	An Incorrect Authorization vulnerability was identified in GitHub Enterprise Server that allowed an authenticated user with a classic personal access token (PAT) lacking the repo scope to retrieve issues and commits from private and internal repositories via the search REST API endpoints. The user must have had existing access to the repository through organization membership or as a collaborator for the vulnerability to be exploitable. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.20 and was fixed in versions 3.16.15, 3.17.12, 3.18.6 and 3.19.3. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2026-29119	International Datacasting Corporation (IDC) SFX Series SuperFlex(SFX2100) SatelliteReceiver contains hardcoded and insecure credentials for the `admin` account. A remote unauthenticated attacker can use these undocumented credentials to access the satellite system directly via the Telnet service, leading to potential system compromise.	N/A	More Details
CVE-2026-31812	Quinn is a pure-Rust, async-compatible implementation of the IETF QUIC transport protocol. Prior to 0.11.14, a remote, unauthenticated attacker can trigger a denial of service in applications using vulnerable quinn versions by sending a crafted QUIC Initial packet containing malformed quic_transport_parameters. In quinn-proto parsing logic, attacker-controlled varints are decoded with unwrap(), so truncated encodings cause Err(UnexpectedEnd) and panic. This is reachable over the network with a single packet and no prior trust or authentication. This vulnerability is fixed in 0.11.14.	N/A	More Details
CVE-2025-70128	A Stored Cross-Site Scripting (XSS) vulnerability exists in the PluXml article comments feature for PluXml versions 5.8.22 and earlier. The application fails to properly sanitize or validate user-supplied input in the "link" field of a comment. An attacker can inject arbitrary JavaScript code using a <script> element. The injected payload is stored in the database and subsequently rendered in the Administration panel's "Comments" section when administrators review submitted comments. Importantly, the malicious script is not reflected in the public-facing comments interface, but only within the backend administration view. Alternatively, users of Administrator, Moderator, Manager roles can also directly input crafted payloads into existing comments. This makes the vulnerability a persistent XSS issue targeting administrative users. This affects /core/admin/comments.php, while CVE-2022-24585 affects /core/admin/comment.php, a uniquely distinct vulnerability.	N/A	More Details
CVE-2026-3370	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-31826	pypdf is a free and open-source pure-python PDF library. Prior to 6.8.0, an attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires parsing a content stream with a rather large /Length value, regardless of the actual data length inside the stream. This vulnerability is fixed in 6.8.0.	N/A	More Details
CVE-2025-20027	Improper input validation in the UEFI WheaERST module for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and	N/A	More Details

	availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2026-28715	Sensitive information disclosure due to improper authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-28720	Unauthorized modification of settings due to insufficient authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-31837	Istio is an open platform to connect, manage, and secure microservices. Prior to 1.29.1, 1.28.5, and 1.27.8, a user of Istio is impacted if the JWKS resolver becomes unavailable or the fetch fails, exposing hardcoded defaults regardless of use of the RequestAuthentication resource. This vulnerability is fixed in 1.29.1, 1.28.5, and 1.27.8.	N/A	More Details
CVE-2026-28714	Unnecessary transmission of sensitive cryptographic material. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-3315	Incorrect Default Permissions, : Execution with Unnecessary Privileges, : Incorrect Permission Assignment for Critical Resource vulnerability in ASSA ABLOY Visionline on Windows allows Configuration/Environment Manipulation.This issue affects Visionline: from 1.0 before 1.33.	N/A	More Details
CVE-2026-31838	Istio is an open platform to connect, manage, and secure microservices. Prior to 1.29.1, 1.28.5, and 1.27.8, a vulnerability in Envoy RBAC header matching could allow authorization policy bypass when policies rely on HTTP headers that may contain multiple values. An attacker could craft requests with multiple header values in a way that causes Envoy to evaluate the header differently than intended, potentially bypassing authorization checks. This may allow unauthorized requests to reach protected services when policies depend on such header-based matching conditions. This vulnerability is fixed in 1.29.1, 1.28.5, and 1.27.8.	N/A	More Details
CVE-2025-20005	Improper buffer restrictions in some UEFI firmware for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (high) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2025-20028	Time-of-check time-of-use race condition in the WheaERST SMM module for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	N/A	More Details
CVE-2026-28716	Information disclosure and manipulation due to improper authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-30967	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.9. and 8.6.22, the OAuth2 authentication adapter, when configured without the useridField option, only verifies that a token is active via the provider's token introspection endpoint, but does not verify that the token belongs to the user identified by authData.id. An attacker with any valid OAuth2 token from the same provider can authenticate as any other user. This affects any Parse Server deployment that uses the generic OAuth2 authentication adapter (configured with oauth2: true) without setting the useridField option. This vulnerability is fixed in 9.5.2-alpha.9. and 8.6.22.	N/A	More Details
CVE-2026-30965	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.8 and 8.6.21, a vulnerability in Parse Server's query handling allows an authenticated or unauthenticated attacker to exfiltrate session tokens of other users by exploiting the redirectClassNameForKey query parameter. Exfiltrated session tokens can be used to take over user accounts. The vulnerability requires the attacker to be able to create or update an object with a new relation field, which depends on the Class-Level Permissions of at least one class. This vulnerability is fixed in 9.5.2-alpha.8 and 8.6.21.	N/A	More Details

CVE-2026-3306	An improper authorization vulnerability was identified in GitHub Enterprise Server that allowed a user with read access to a repository and write access to a project to modify issue and pull request metadata through the project. When adding an item to a project that already existed, column value updates were applied without verifying the actor's repository write permissions. This vulnerability was reported via the GitHub Bug Bounty program and has been fixed in GitHub Enterprise Server versions 3.14.24, 3.15.19, 3.16.15, 3.17.12, 3.18.6 and 3.19.3.	N/A	More Details
CVE-2026-0120	In modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-30962	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.6 and 8.6.19, the validation for protected fields only checks top-level query keys. By wrapping a query constraint on a protected field inside a logical operator, the check is bypassed entirely. This allows any authenticated user to query on protected fields to extract field values. All Parse Server deployments have default protected fields and are vulnerable. This vulnerability is fixed in 9.5.2-alpha.6 and 8.6.19.	N/A	More Details
CVE-2025-20064	Improper input validation in the UEFI FlashUcAcmSmm module for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (high) impacts.	N/A	More Details
CVE-2026-30954	LinkAce is a self-hosted archive to collect website links. In 2.1.0 and earlier, the processTaxonomy() method in LinkRepository.php allows authenticated users to attach other users' private tags and lists to their own links by passing integer IDs.	N/A	More Details
CVE-2026-30972	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior o 9.5.2-alpha.10 and 8.6.23, Parse Server's rate limiting middleware is applied at the Express middleware layer, but the batch request endpoint (/batch) processes sub-requests internally by routing them directly through the Promise router, bypassing Express middleware including rate limiting. An attacker can bundle multiple requests targeting a rate-limited endpoint into a single batch request to circumvent the configured rate limit. Any Parse Server deployment that relies on the built-in rate limiting feature is affected. This vulnerability is fixed in 9.5.2-alpha.10 and 8.6.23.	N/A	More Details
CVE-2026-3854	An improper neutralization of special elements vulnerability was identified in GitHub Enterprise Server that allowed an attacker with push access to a repository to achieve remote code execution on the instance. During a git push operation, user-supplied push option values were not properly sanitized before being included in internal service headers. Because the internal header format used a delimiter character that could also appear in user input, an attacker could inject additional metadata fields through crafted push option values. This vulnerability was reported via the GitHub Bug Bounty program and has been fixed in GitHub Enterprise Server versions 3.14.24, 3.15.19, 3.16.15, 3.17.12, 3.18.6 and 3.19.3.	N/A	More Details
CVE-2026-28726	Sensitive information disclosure due to improper access control. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-0117	In mfc_dec_dqbuf of mfc_dec_v4l2.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-31809	SiYuan is a personal knowledge management system. Prior to 3.5.10, SiYuan's SVG sanitizer (SanitizeSVG) checks href attributes for the javascript: prefix using strings.HasPrefix(). However, inserting ASCII tab (&#9;), newline (&#10;), or carriage return (&#13;) characters inside the javascript: string bypasses this prefix check. Browsers strip these characters per the WHATWG URL specification before parsing the URL scheme, so the JavaScript still executes. This allows an attacker to inject executable JavaScript into the unauthenticated /api/icon/getDynamicIcon endpoint, creating a reflected XSS. This is a second bypass of the fix for CVE-2026-29183 (fixed in v3.5.9). This vulnerability is fixed in 3.5.10.	N/A	More Details
CVE-2026-31827	Alienbin is an anonymous code and text sharing web service. In 1.0.0 and earlier, the /save endpoint in server.js drops and recreates the MongoDB TTL index on the entire post collection for every new paste submission. When User B submits a paste with a short TTL (e.g., 30 seconds), the TTL index is recreated with expireAfterSeconds: 30 for all documents in the collection. This causes User A's paste (originally set to 7 days) to be deleted after 30 seconds. An attacker can intentionally delete all	N/A	More Details

	existing pastes by repeatedly submitting pastes with ttlOption=30s.		
CVE-2026-0116	In __mfc_handle_released_buf of mfc_core_isr.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-31828	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.13 and 8.6.26, the LDAP authentication adapter is vulnerable to LDAP injection. User-supplied input (authData.id) is interpolated directly into LDAP Distinguished Names (DN) and group search filters without escaping special characters. This allows an attacker with valid LDAP credentials to manipulate the bind DN structure and to bypass group membership checks. This enables privilege escalation from any authenticated LDAP user to a member of any restricted group. The vulnerability affects Parse Server deployments that use the LDAP authentication adapter with group-based access control. This vulnerability is fixed in 9.5.2-alpha.13 and 8.6.26.	N/A	More Details
CVE-2026-28722	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Cyber Protect 17 (Windows) before build 41186.	N/A	More Details
CVE-2026-28721	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Cyber Protect 17 (Windows) before build 41186.	N/A	More Details
CVE-2026-28727	Local privilege escalation due to insecure Unix socket permissions. The following products are affected: Acronis Cyber Protect 17 (macOS) before build 41186, Acronis Cyber Protect Cloud Agent (macOS) before build 41124.	N/A	More Details
CVE-2026-31807	SiYuan is a personal knowledge management system. Prior to 3.5.10, SiYuan's SVG sanitizer (SanitizeSVG) blocks dangerous elements (<script>, <iframe>, <foreignobject>) and removes on* event handlers and javascript: in href attributes. However, it does NOT block SVG animation elements (<animate>, <set>) which can dynamically set attributes to dangerous values at runtime, bypassing the static sanitization. This allows an attacker to inject executable JavaScript into the unauthenticated /api/icon/getDynamicIcon endpoint (type=8), creating a reflected XSS. This is a bypass of the fix for CVE-2026-29183 (fixed in v3.5.9). This vulnerability is fixed in v3.5.10.	N/A	More Details
CVE-2026-3862	Cross-site Scripting (XSS) allows an attacker to submit specially crafted data to the application which is returned unaltered in the resulting web page.	N/A	More Details
CVE-2026-28724	Unauthorized data access due to insufficient access control validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-0118	In oobconfig, there is a possible bypass of carrier restrictions due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2026-26742	PX4 Autopilot versions 1.12.x through 1.15.x contain a protection mechanism failure in the "Re-arm Grace Period" logic. The system incorrectly applies the in-air emergency re-arm logic to ground scenarios. If a pilot switches to Manual mode and re-arms within 5 seconds (default configuration) of an automatic landing, the system bypasses all pre-flight safety checks, including the throttle threshold check. This allows for an immediate high-thrust takeoff if the throttle stick is raised, leading to loss of control.	N/A	More Details
CVE-2026-26741	PX4 Autopilot versions 1.12.x through 1.15.x contain a logic flaw in the mode switching mechanism. When switching from Auto mode to Manual mode while the drone is in the "ARMED" state (after landing and before the automatic disarm triggered by the COM_DISARM_LAND parameter), the system lacks a throttle threshold safety check for the physical throttle stick. This flaw can directly cause the drone to lose control, experience rapid uncontrolled ascent (flyaway), and result in property damage	N/A	More Details
CVE-2026-0119	In usim_SendMCCMNCIndMsg of usim_Registration.c, there is a possible out of bounds write due to memory corruption. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
	Sylius is an Open Source eCommerce Framework on Symfony. An authenticated Insecure Direct Object Reference (IDOR) vulnerability exists in multiple shop LiveComponents due to unvalidated resource IDs accepted via #[LiveArg] parameters. Unlike props, which are protected by LiveComponent's @checksum, args are fully user-controlled - any action that accepts a resource ID via #[LiveArg] and loads it with ->find() without ownership validation is vulnerable. Checkout address FormComponent		

CVE-2026-31820	(addressFieldUpdated action): Accepts an addressId via #[LiveArg] and loads it without verifying ownership, exposing another user's first name, last name, company, phone number, street, city, postcode, and country. Cart WidgetComponent (refreshCart action): Accepts a cartId via #[LiveArg] and loads any order directly from the repository, exposing order total and item count. Cart SummaryComponent (refreshCart action): Accepts a cartId via #[LiveArg] and loads any order directly from the repository, exposing subtotal, discount, shipping cost, taxes (excluded and included), and order total. Since sylius_order contains both active carts (state=cart) and completed orders (state=new/fulfilled) in the same ID space, the cart IDOR exposes data from all orders, not just active carts. The issue is fixed in versions: 2.0.16, 2.1.12, 2.2.3 and above.	N/A	More Details
CVE-2026-31800	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.12 and 8.6.25, the _GraphQLConfig and _Audience internal classes can be read, modified, and deleted via the generic /classes/_GraphQLConfig and /classes/_Audience REST API routes without master key authentication. This bypasses the master key enforcement that exists on the dedicated /graphql-config and /push_audiences endpoints. An attacker can read, modify and delete GraphQL configuration and push audience data. This vulnerability is fixed in 9.5.2-alpha.12 and 8.6.25.	N/A	More Details
CVE-2026-30946	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior 9.5.2-alpha.2 and 8.6.15, an unauthenticated attacker can exhaust Parse Server resources (CPU, memory, database connections) through crafted queries that exploit the lack of complexity limits in the REST and GraphQL APIs. All Parse Server deployments using the REST or GraphQL API are affected. This vulnerability is fixed in 9.5.2-alpha.2 and 8.6.15.	N/A	More Details
CVE-2026-30846	Wekan is an open source kanban tool built with Meteor. In versions 8.31.0 through 8.33, the globalwebhooks publication exposes all global webhook integrations—including sensitive url and token fields—without performing any authentication check on the server side. Although the subscription is normally invoked from the admin settings page, the server-side publication has no access control, meaning any DDP client, including unauthenticated ones, can subscribe and receive the data. This allows an unauthenticated attacker to retrieve global webhook URLs and authentication tokens, potentially enabling unauthorized use of those webhooks and access to connected external services. This issue has been fixed in version 8.34.	N/A	More Details
CVE-2026-30942	Flare is a Next.js-based, self-hostable file sharing platform that integrates with screenshot tools. Prior to 1.7.3, an authenticated path traversal vulnerability in /api/avatars/[filename] allows any logged-in user to read arbitrary files from within the application container. The filename URL parameter is passed to path.join() without sanitization, and getFileStream() performs no path validation, enabling %2F-encoded ../ sequences to escape the uploads/avatars/ directory and read any file accessible to the nextjs process under /app/. Authentication is enforced by Next.js middleware. However, on instances with open registration enabled (the default), any attacker can self-register and immediately exploit this. This vulnerability is fixed in 1.7.3.	N/A	More Details
CVE-2026-29063	Immutable.js provides many Persistent Immutable data structures. Prior to versions 3.8.3, 4.3.7, and 5.1.5, Prototype Pollution is possible in immutable via the mergeDeep(), mergeDeepWith(), merge(), Map.toJS(), and Map.toObject() APIs. This issue has been patched in versions 3.8.3, 4.3.7, and 5.1.5.	N/A	More Details
CVE-2026-28133	Unrestricted Upload of File with Dangerous Type vulnerability in WP Chill Filr filr-protection allows Upload a Web Shell to a Web Server.This issue affects Filr: from n/a through <= 1.2.12.	N/A	More Details
CVE-2026-30833	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to versions 7.10.8, 7.11.5, 7.12.5, 7.13.4, 8.0.2, 8.1.1, and 8.2.0, a NoSQL injection vulnerability exists in Rocket.Chat's account service used in the ddp-streamer micro service that allows unauthenticated attackers to manipulate MongoDB queries during authentication. The vulnerability is located in the username-based login flow where user-supplied input is directly embedded into a MongoDB query selector without validation. An attacker can inject MongoDB operator expressions (e.g., { $regex: '.*' }) in place of a username string, causing the database query to match unintended user records. This issue has been patched in versions 7.10.8, 7.11.5, 7.12.5, 7.13.4, 8.0.2, 8.1.1, and 8.2.0.	N/A	More Details
CVE-2025-69650	GNU Binutils thru 2.46 readelf contains a double free vulnerability when processing a crafted ELF binary with malformed relocation data. During GOT relocation handling, dump_relocations may return early without initializing the all_relocations array. As a result, process_got_section_contents() may pass an uninitialized r_symbol pointer to free(), leading to a double free and terminating the program with SIGABRT. No evidence of exploitable memory corruption or code execution was observed; the impact is limited to denial of service.	N/A	More Details
CVE-2025-69653	A crafted JavaScript input can trigger an internal assertion failure in QuickJS release 2025-09-13, fixed in commit 1dbba8a88eaa40d15a8a9b70bb1a0b8fb5b552e6 (2025-12-11), in file gc_decref_child in quickjs.c, when executed with the qjs interpreter using the -m option. This leads to an abort (SIGABRT)	N/A	More Details

	during garbage collection and causes a denial-of-service.		
CVE-2026-30852	Caddy is an extensible server platform that uses TLS by default. From version 2.7.5 to before version 2.11.2, the vars_regexp matcher in vars.go:337 double-expands user-controlled input through the Caddy replacer. When vars_regexp matches against a placeholder like {http.request.header.X-Input}, the header value gets resolved once (expected), then passed through repl.ReplaceAll() again (the bug). This means an attacker can put {env.DATABASE_URL} or {file./etc/passwd} in a request header and the server will evaluate it, leaking environment variables, file contents, and system info. This issue has been patched in version 2.11.2.	N/A	More Details
CVE-2026-29196	Netmaker makes networks with WireGuard. Prior to version 1.5.0, a user assigned the platform-user role can retrieve WireGuard private keys of all wireguard configs in a network by calling GET /api/extclients/{network} or GET /api/nodes/{network}. While the Netmaker UI restricts visibility, the API endpoints return full records, including private keys, without filtering based on the requesting user's ownership. This issue has been patched in version 1.5.0.	N/A	More Details
CVE-2026-29195	Netmaker makes networks with WireGuard. Prior to version 1.5.0, the user update handler (PUT /api/users/{username}) lacks validation to prevent an admin-role user from assigning the super-admin role during account updates. While the code correctly blocks an admin from assigning the admin role to another user, it does not include an equivalent check for the super-admin role. This issue has been patched in version 1.5.0.	N/A	More Details
CVE-2026-30838	league/commonmark is a PHP Markdown parser. Prior to version 2.8.1, the DisallowedRawHtml extension can be bypassed by inserting a newline, tab, or other ASCII whitespace character between a disallowed HTML tag name and the closing >. For example, <script\n> would pass through unfiltered and be rendered as a valid HTML tag by browsers. This is a cross-site scripting (XSS) vector for any application that relies on this extension to sanitize untrusted user input. All applications using the DisallowedRawHtml extension to process untrusted markdown are affected. Applications that use a dedicated HTML sanitizer (such as HTML Purifier) on the rendered output are not affected. This issue has been patched in version 2.8.1.	N/A	More Details
CVE-2026-29786	node-tar is a full-featured Tar for Node.js. Prior to version 7.5.10, tar can be tricked into creating a hardlink that points outside the extraction directory by using a drive-relative link target such as C:../target.txt, which enables file overwrite outside cwd during normal tar.x() extraction. This issue has been patched in version 7.5.10.	N/A	More Details
CVE-2026-29178	Lemmy, a link aggregator and forum for the fediverse, is vulnerable to server-side request forgery via a dependency on activitypub_federation, a framework for ActivityPub federation in Rust. Prior to version 0.19.16, the GET /api/v4/image/{filename} endpoint is vulnerable to unauthenticated SSRF through parameter injection in the file_type query parameter. An attacker can inject arbitrary query parameters into the internal request to pict-rs, including the proxy parameter which causes pict-rs to fetch arbitrary URLs. This issue has been patched in version 0.19.16.	N/A	More Details
CVE-2026-3653	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-29781	Sliver is a command and control framework that uses a custom Wireguard netstack. In versions from 1.7.3 and prior, a vulnerability exists in the Sliver C2 server's Protobuf unmarshalling logic due to a systemic lack of nil-pointer validation. By extracting valid implant credentials and omitting nested fields in a signed message, an authenticated actor can trigger an unhandled runtime panic. Because the mTLS, WireGuard, and DNS transport layers lack the panic recovery middleware present in the HTTP transport, this results in a global process termination. While requiring post-authentication access (a captured implant), this flaw effectively acts as an infrastructure "kill-switch," instantly severing all active sessions across the entire fleet and requiring a manual server restart to restore operations. At time of publication, there are no publicly available patches.	N/A	More Details
CVE-2025-69654	A crafted JavaScript input executed with the QuickJS release 2025-09-13, fixed in commit fcd33c1afa7b3028531f53cd1190a3877454f6b3 (2025-12-11),`qjs` interpreter using the `-m` option and a low memory limit can cause an out-of-memory condition followed by an assertion failure in JS_FreeRuntime (list_empty(&rt->gc_obj_list)) during runtime cleanup. Although the engine reports an OOM error, it subsequently aborts with SIGABRT because the GC object list is not fully released. This results in a denial of service.	N/A	More Details
	Wekan is an open source kanban tool built with Meteor. Versions 8.32 and 8.33 have a critical Insecure Direct Object Reference (IDOR) issue which could allow unauthorized users to modify custom fields across boards through its custom fields update endpoints, potentially leading to unauthorized data manipulation. The PUT /api/boards/:boardId/custom-fields/:customFieldId endpoint in Wekan validates that the authenticated user has access to the specified boardId, but the subsequent database update		

CVE-2026-30843	uses only the custom field's _id as a filter without confirming the field actually belongs to that board. This means an attacker who owns any board can modify custom fields on any other board by supplying a foreign custom field ID, and the same flaw exists in the POST, PUT, and DELETE endpoints for dropdown items under custom fields. The required custom field IDs can be obtained by exporting a board (which only needs read access), since the exported JSON includes the IDs of all board components. The authorization check is performed against the wrong resource, allowing cross-board custom field manipulation. This issue has been fixed in version 8.34.	N/A	More Details
CVE-2026-29771	Netmaker makes networks with WireGuard. Prior to version 1.2.0, the /api/server/shutdown endpoint allows termination of the Netmaker server process via syscall.SIGINT. This allows any user to repeatedly shut down the server, causing cyclic denial of service with approximately 3-second restart intervals. This issue has been patched in version 1.2.0.	N/A	More Details
CVE-2026-29194	Netmaker makes networks with WireGuard. Prior to version 1.5.0, the Authorize middleware in Netmaker incorrectly validates host JWT tokens. When a route permits host authentication (hostAllowed=true), a valid host token bypasses all subsequent authorization checks without verifying that the host is authorized to access the specific requested resource. Any entity possessing knowledge of object identifiers (node IDs, host IDs) can craft a request with an arbitrary valid host token to access, modify, or delete resources belonging to other hosts. Affected endpoints include node info retrieval, host deletion, MQTT signal transmission, fallback host updates, and failover operations. This issue has been patched in version 1.5.0.	N/A	More Details
CVE-2026-21628	A improperly secured file management feature allows uploads of dangerous data types for unauthenticated users, leading to remote code execution.	N/A	More Details
CVE-2026-3236	In affected versions of Octopus Server it was possible to create a new API key from an existing access token resulting in the new API key having a lifetime exceeding the original API key used to mint the access token.	N/A	More Details
CVE-2026-30831	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to versions 7.10.8, 7.11.5, 7.12.5, 7.13.4, 8.0.2, 8.1.1, and 8.2.0, authentication vulnerabilities exist in Rocket.Chat's enterprise DDP Streamer service. The Account.login method exposed through the DDP Streamer does not enforce Two-Factor Authentication (2FA) or validate user account status (deactivated users can still login), despite these checks being mandatory in the standard Meteor login flow. This issue has been patched in versions 7.10.8, 7.11.5, 7.12.5, 7.13.4, 8.0.2, 8.1.1, and 8.2.0.	N/A	More Details
CVE-2026-28514	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to versions 7.8.6, 7.9.8, 7.10.7, 7.11.4, 7.12.4, 7.13.3, and 8.0.0, a critical authentication bypass vulnerability exists in Rocket.Chat's account service used in the ddp-streamer micro service that allows an attacker to log in to the service as any user with a password set, using any arbitrary password. The vulnerability stems from a missing await keyword when calling an asynchronous password validation function, causing a Promise object (which is always truthy) to be evaluated instead of the actual boolean validation result. This may lead to account takeover of any user whose username is known or guessable. This issue has been patched in versions 7.8.6, 7.9.8, 7.10.7, 7.11.4, 7.12.4, 7.13.3, and 8.0.0.	N/A	More Details
CVE-2024-14027	In the Linux kernel, the following vulnerability has been resolved: fs/xattr: missing fdput() in fremovexattr error path In the Linux kernel, the fremovexattr() syscall calls fdget() to acquire a file reference but returns early without calling fdput() when strncpy_from_user() fails on the name argument. In multi-threaded processes where fdget() takes the slow path, this permanently leaks one file reference per call, pinning the struct file and associated kernel objects in memory. An unprivileged local user can exploit this to cause kernel memory exhaustion. The issue was inadvertently fixed by commit a71874379ec8 ("xattr: switch to CLASS(fd)").	N/A	More Details
CVE-2026-21622	Insufficient Session Expiration vulnerability in hexpm hexpm ('Elixir.Hexpm.Accounts.PasswordReset' module) allows Account Takeover. Password reset tokens generated via the "Reset your password" flow do not expire. When a user requests a password reset, Hex sends an email containing a reset link with a token. This token remains valid indefinitely until used. There is no time-based expiration enforced. If a user's historical emails are exposed through a data breach (e.g., a leaked mailbox archive), any unused password reset email contained in that dataset could be used by an attacker to reset the victim's password. The attacker does not need current access to the victim's email account, only access to a previously leaked copy of the reset email. This vulnerability is associated with program files lib/hexpm/accounts/password_reset.ex and program routines 'Elixir.Hexpm.Accounts.PasswordReset':can_reset?/3. This issue affects hexpm: from 617e44c71f1dd9043870205f371d375c5c4d886d before bb0e42091995945deef10556f58d046a52eb7884.	N/A	More Details

CVE-2026-26034	UPS Multi-UPS Management Console (MUMC) version 01.06.0001 (A03) contains an Incorrect Default Permissions (CWE-276) vulnerability that allows an attacker to execute arbitrary code with SYSTEM privileges by causing the application to load a specially crafted DLL.	N/A	More Details
CVE-2025-70059	An issue pertaining to CWE-400: Uncontrolled Resource Consumption was discovered in YMFE yapi v1.12.0 and allows attackers to cause a denial of service.	N/A	More Details
CVE-2026-3089	Actual Sync Server allows authenticated users to upload files through POST /sync/upload-user-file. In versions prior to 26.3.0, improper validation of the user-controlled x-actual-file-id header means that traversal segments (../) can escape the intended directory and write files outside userFiles.This issue affects prior versions of Actual Sync Server 26.3.0.	N/A	More Details
CVE-2026-2261	Due to a programming error, blocklistd leaks a socket descriptor for each adverse event report it receives. Once a certain number of leaked sockets is reached, blocklistd becomes unable to run the helper script: a child process is forked, but this child dereferences a null pointer and crashes before it is able to exec the helper. At this point, blocklistd still records adverse events but is unable to block new addresses or unblock addresses whose database entries have expired. Once a second, much higher number of leaked sockets is reached, blocklistd becomes unable to receive new adverse event reports. An attacker may take advantage of this by triggering a large number of adverse events from sacrificial IP addresses to effectively disable blocklistd before launching an attack. Even in the absence of attacks or probes by would-be attackers, adverse events will occur regularly in the course of normal operations, and blocklistd will gradually run out file descriptors and become ineffective. The accumulation of open sockets may have knock-on effects on other parts of the system, resulting in a general slowdown until blocklistd is restarted.	N/A	More Details
CVE-2026-28718	Denial of service due to insufficient input validation in authentication logging. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-22405	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Overton overton allows PHP Local File Inclusion.This issue affects Overton: from n/a through <= 1.3.	N/A	More Details
CVE-2025-33022	Rejected reason: The reporter agreed to not assign CVE ID	N/A	More Details
CVE-2026-27339	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Buzz Stone | Magazine & Viral Blog WordPress Theme buzzstone allows PHP Local File Inclusion.This issue affects Buzz Stone | Magazine & Viral Blog WordPress Theme: from n/a through <= 1.0.2.	N/A	More Details
CVE-2026-28443	OpenReplay is a self-hosted session replay suite. Prior to version 1.20.0, the POST /{projectId}/cards/search endpoint has a SQL injection in the sort.field parameter. This issue has been patched in version 1.20.0.	N/A	More Details
CVE-2026-29783	The shell tool within GitHub Copilot CLI versions prior to and including 0.0.422 can allow arbitrary code execution through crafted bash parameter expansion patterns. An attacker who can influence the commands executed by the agent (e.g., via prompt injection through repository files, MCP server responses, or user instructions) can exploit bash parameter transformation operators to execute hidden commands, bypassing the safety assessment that classifies commands as "read-only." This has been patched in version 0.0.423. The vulnerability stems from how the CLI's shell safety assessment evaluates commands before execution. The safety layer parses and classifies shell commands as either read-only (safe) or write-capable (requires user approval). However, several bash parameter expansion features can embed executable code within arguments to otherwise read-only commands, causing them to appear safe while actually performing arbitrary operations. The specific dangerous patterns are ${var@P}, ${var=value} / ${var:=value}, ${!var}, and nested $(cmd) or <(cmd) inside ${...} expansions. An attacker who can influence command text sent to the shell tool - for example, through prompt injection via malicious repository content (README files, code comments, issue bodies), compromised or malicious MCP server responses, or crafted user instructions containing obfuscated commands - could achieve arbitrary code execution on the user's workstation. This is possible even in permission modes that require user approval for write operations, since the commands can appear to use only read-only utilities to ultimately trigger write operations. Successful exploitation could lead to data exfiltration, file modification, or further system compromise.	N/A	More Details
	NLTK versions <=3.9.2 are vulnerable to arbitrary code execution due to improper input validation in the StanfordSegmenter module. The module dynamically loads external Java .jar files without		

CVE-2026-0848	verification or sandboxing. An attacker can supply or replace the JAR file, enabling the execution of arbitrary Java bytecode at import time. This vulnerability can be exploited through methods such as model poisoning, MITM attacks, or dependency poisoning, leading to remote code execution. The issue arises from the direct execution of the JAR file via subprocess with unvalidated classpath input, allowing malicious classes to execute when loaded by the JVM.	N/A	More Details
CVE-2022-4947	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-32111. Reason: This candidate is a reservation duplicate of CVE-2024-32111. Notes: All CVE users should reference CVE-2024-32111 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-1799	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate has been determined not to be a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-28353	Trivy Vulnerability Scanner is a VS Code extension that helps find vulnerabilities. In Trivy VSCode Extension version 1.8.12, which was distributed via OpenVSX marketplace was compromised and contained malicious code designed to leverage local AI coding agent to collect and exfiltrate sensitive information. Users using the affected artifact are advised to immediately remove it and rotate environment secrets. The malicious artifact has been removed from the marketplace. No other affected artifacts have been identified.	N/A	More Details
CVE-2026-30896	The installer for Qsee Client versions 1.0.1 and prior insecurely load Dynamic Link Libraries (DLLs). When a user is directed to place some malicious DLL to the same directory and execute the affected installer, then arbitrary code may be executed with the administrative privilege.	N/A	More Details
CVE-2026-27123	Rejected reason: Reason: This candidate was issued in error.	N/A	More Details
CVE-2026-21621	Incorrect Authorization vulnerability in hexpm hexpm/hexpm ('Elixir.HexpmWeb.API.OAuthController' module) allows Privilege Escalation. An API key created with read-only permissions (domain: "api", resource: "read") can be escalated to full write access under specific conditions. When exchanging a read-only API key via the OAuth client_credentials grant, the resource qualifier is ignored. The resulting JWT receives the broad "api" scope instead of the expected "api:read" scope. This token is therefore treated as having full API access. If an attacker is able to obtain a victim's read-only API key and a valid 2FA (TOTP) code for the victim account, they can use the incorrectly scoped JWT to create a new full-access API key with unrestricted API permissions that does not expire by default and can perform write operations such as publishing, retiring, or modifying packages. This vulnerability is associated with program files lib/hexpm_web/controllers/api/oauth_controller.ex and program routines 'Elixir.HexpmWeb.API.OAuthController':validate_scopes_against_key/2. This issue affects hexpm: from 71829cb6f6559bcceb1ef4e43a2fb8cdd3af654b before 71c127afebb7ed7cc637eb231b98feb802d62999.	N/A	More Details
CVE-2025-13350	Ubuntu Linux 6.8 GA retains the legacy AF_UNIX garbage collector but backports upstream commit 8594d9b85c07 ("af_unix: Don’t call skb_get() for OOB skb"). When orphaned MSG_OOB sockets hit unix_gc(), the garbage collector still calls kfree_skb() as if OOB SKBs held two references; on Ubuntu Linux 6.8 (Noble Numbat) kernel tree, they have only the queue reference, so the buffer is freed while still reachable and subsequent queue walks dereference freed memory, yielding a reliable local privilege escalation (LPE) caused by a use-after-free (UAF). Ubuntu builds that have already taken the new GC stack from commit 4090fa373f0e, and mainline Linux kernels shipping that infrastructure are unaffected because they no longer execute the legacy collector path. This issue affects Ubuntu Linux from 6.8.0-56.58 before 6.8.0-84.84.	N/A	More Details
CVE-2025-69534	Python-Markdown version 3.8 contain a vulnerability where malformed HTML-like sequences can cause html.parser.HTMLParser to raise an unhandled AssertionError during Markdown parsing. Because Python-Markdown does not catch this exception, any application that processes attacker-controlled Markdown may crash. This enables remote, unauthenticated Denial of Service in web applications, documentation systems, CI/CD pipelines, and any service that renders untrusted Markdown. The issue was acknowledged by the vendor and fixed in version 3.8.1. This issue causes a remote Denial of Service in any application parsing untrusted Markdown, and can lead to Information Disclosure through uncaught exceptions.	N/A	More Details
CVE-2026-30791	Use of a Broken or Risky Cryptographic Algorithm vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android, WebClient (Config import, URI scheme handler, CLI --config modules) allows Retrieve Embedded Sensitive Data. This vulnerability is associated with program files flutter/lib/common.Dart, hbb_common/src/config.Rs and program routines parseRustdeskUri(), importConfig(). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details

CVE-2026-3598	Use of a Broken or Risky Cryptographic Algorithm vulnerability in rustdesk-server-pro RustDesk Server Pro rustdesk-server-pro on Windows, MacOS, Linux (Config string generation, web console export modules) allows Retrieve Embedded Sensitive Data. This vulnerability is associated with program routines Config export/generation routines. This issue affects RustDesk Server Pro: through 1.7.5.	N/A	More Details
CVE-2026-30844	Wekan is an open source kanban tool built with Meteor. Versions 8.32 and 8.33 are vulnerable to Server-Side Request Forgery (SSRF) via attachment URL loading. During board import in Wekan, attachment URLs from user-supplied JSON data are fetched directly by the server without any URL validation or filtering, affecting both the Wekan and Trello import flows. The parseActivities() and parseActions() methods extract user-controlled attachment URLs, which are then passed directly to Attachments.load() for download with no sanitization. This Server-Side Request Forgery (SSRF) vulnerability allows any authenticated user to make the server issue arbitrary HTTP requests, potentially accessing internal network services such as cloud instance metadata endpoints (exposing IAM credentials), internal databases, and admin panels that are otherwise unreachable from outside the network. This issue has been fixed in version 8.34.	N/A	More Details
CVE-2026-30793	Cross-Site Request Forgery (CSRF) vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (Flutter URI scheme handler, FFI bridge modules) allows Privilege Escalation. This vulnerability is associated with program files flutter/lib/common.Dart, src/flutter_ffi.Rs and program routines URI handler for rustdesk://password/, bind.MainSetPermanentPassword(). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30241	Mercurius is a GraphQL adapter for Fastify. Prior to version 16.8.0, Mercurius fails to enforce the configured queryDepth limit on GraphQL subscription queries received over WebSocket connections. The depth check is correctly applied to HTTP queries and mutations, but subscription queries are parsed and executed without invoking the depth validation. This allows a remote client to submit arbitrarily deeply nested subscription queries over WebSocket, bypassing the intended depth restriction. On schemas with recursive types, this can lead to denial of service through exponential data resolution on each subscription event. This issue has been patched in version 16.8.0.	N/A	More Details
CVE-2026-30238	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.155, 25.0.88, and 26.0.10, there is a reflected XSS vulnerability in GroupOffice on the external/index flow. The f parameter (Base64 JSON) is decoded and then injected into an inline JavaScript block without strict escaping, allowing </script><script>...</script> injection and arbitrary JavaScript execution in the victim's browser. This issue has been patched in versions 6.8.155, 25.0.88, and 26.0.10.	N/A	More Details
CVE-2026-30237	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.155, 25.0.88, and 26.0.10, there is a reflected XSS vulnerability in the GroupOffice installer, endpoint install/license.php. The POST field license is rendered without escaping inside a <textarea>, allowing a </textarea><script>...</script> breakout.. This issue has been patched in versions 6.8.155, 25.0.88, and 26.0.10.	N/A	More Details
CVE-2026-30794	Improper Certificate Validation vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (HTTP API client, TLS transport modules) allows Adversary in the Middle (AiTM). This vulnerability is associated with program files src/hbbs_http/http_client.Rs and program routines TLS retry with danger_accept_invalid_certs(true). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30795	Cleartext Transmission of Sensitive Information vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (Heartbeat sync loop modules) allows Sniffing Attacks. This vulnerability is associated with program files src/hbbs_http/sync.Rs and program routines Heartbeat JSON payload construction (preset-address-book-password). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30796	Cleartext Transmission of Sensitive Information vulnerability in rustdesk-server-pro RustDesk Server Pro rustdesk-server-pro on Windows, MacOS, Linux (Address book sync API modules) allows Sniffing Attacks. This vulnerability is associated with program files Closed source — API endpoint handling heartbeat sync and program routines Heartbeat API handler (accepts preset-address-book-password in plaintext). This issue affects RustDesk Server Pro: through 1.7.5.	N/A	More Details
CVE-2026-30835	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.7 and 9.5.0-alpha.6, malformed $regex query parameter (e.g. [abc) causes the database to return a structured error object that is passed unsanitized through the API response. This leaks database internals such as error messages, error codes, code names, cluster timestamps, and topology details. The vulnerability is exploitable by any client that can send query requests, depending on the deployment's permission configuration. This issue has been patched in versions 8.6.7 and 9.5.0-alpha.6.	N/A	More Details

CVE-2026-30231	Flare is a Next.js-based, self-hostable file sharing platform that integrates with screenshot tools. Prior to version 1.7.2, the raw and direct file routes only block unauthenticated users from accessing private files. Any authenticated, non-owner user who knows the file URL can retrieve the content, which is inconsistent with stricter checks used by other endpoints. This issue has been patched in version 1.7.2.	N/A	More Details
CVE-2026-25048	xgrammar is an open-source library for efficient, flexible, and portable structured generation. Prior to version 0.1.32, the multi-level nested syntax caused a segmentation fault (core dumped). This issue has been patched in version 0.1.32.	N/A	More Details
CVE-2026-30230	Flare is a Next.js-based, self-hostable file sharing platform that integrates with screenshot tools. Prior to version 1.7.2, the thumbnail endpoint does not validate the password for password-protected files. It checks ownership/admin for private files but skips password verification, allowing thumbnail access without the password. This issue has been patched in version 1.7.2.	N/A	More Details
CVE-2026-30229	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.6 and 9.5.0-alpha.4, the readOnlyMasterKey can call POST /loginAs to obtain a valid session token for any user. This allows a read-only credential to impersonate arbitrary users with full read and write access to their data. Any Parse Server deployment that uses readOnlyMasterKey is affected. This issue has been patched in versions 8.6.6 and 9.5.0-alpha.4.	N/A	More Details
CVE-2026-30228	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.5 and 9.5.0-alpha.3, the readOnlyMasterKey can be used to create and delete files via the Files API (POST /files/:filename, DELETE /files/:filename). This bypasses the read-only restriction which violates the access scope of the readOnlyMasterKey. Any Parse Server deployment that uses readOnlyMasterKey and exposes the Files API is affected. An attacker with access to the readOnlyMasterKey can upload arbitrary files or delete existing files. This issue has been patched in versions 8.6.5 and 9.5.0-alpha.3.	N/A	More Details
CVE-2026-30227	MimeKit is a C# library which may be used for the creation and parsing of messages using the Multipurpose Internet Mail Extension (MIME), as defined by numerous IETF specifications. Prior to version 4.15.1, a CRLF injection vulnerability in MimeKit allows an attacker to embed \r\n into the SMTP envelope address local-part (when the local-part is a quoted-string). This is non-compliant with RFC 5321 and can result in SMTP command injection (e.g., injecting additional RCPT TO / DATA / RSET commands) and/or mail header injection, depending on how the application uses MailKit/MimeKit to construct and send messages. The issue becomes exploitable when the attacker can influence a MailboxAddress (MAIL FROM / RCPT TO) value that is later serialized to an SMTP session. RFC 5321 explicitly defines the SMTP mailbox local-part grammar and does not permit CR (13) or LF (10) inside Quoted-string (qtextSMTP and quoted-pairSMTP ranges exclude control characters). SMTP commands are terminated by <CRLF>, making CRLF injection in command arguments particularly dangerous. This issue has been patched in version 4.15.1.	N/A	More Details
CVE-2026-30797	Missing Authorization vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (Flutter URI scheme handler, config import modules) allows Application API Message Manipulation via Man-in-the-Middle. This vulnerability is associated with program files flutter/lib/common.Dart and program routines importConfig() via URI handler. This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-29790	dbt-common is the shared common utilities for dbt-core and adapter implementations use. Prior to versions 1.34.2 and 1.37.3, a path traversal vulnerability exists in dbt-common's safe_extract() function used when extracting tarball archives. The function uses os.path.commonprefix() to validate that extracted files remain within the intended destination directory. However, commonprefix() compares paths character-by-character rather than by path components, allowing a malicious tarball to write files to sibling directories with matching name prefixes. This issue has been patched in versions 1.34.2 and 1.37.3.	N/A	More Details
CVE-2026-29788	TSPortal is the WikiTide Foundation’s in-house platform used by the Trust and Safety team to manage reports, investigations, appeals, and transparency work. Prior to version 30, conversion of empty strings to null allows disguising DPA reports as genuine self-deletion reports. This issue has been patched in version 30.	N/A	More Details
CVE-2026-30845	Wekan is an open source kanban tool built with Meteor. In versions 8.31.0 through 8.33, the board composite publication in Wekan publishes all integration data for a board without any field filtering, exposing sensitive fields including webhook URLs and authentication tokens to any subscriber. Since board publications are accessible to all board members regardless of their role (including read-only and comment-only users), and even to unauthenticated DDP clients for public boards, any user who can access a board can retrieve its webhook credentials. This token leak allows attackers to make unauthenticated requests to the exposed webhooks, potentially triggering unauthorized actions in connected external services. This issue has been fixed in version 8.34.	N/A	More Details

CVE-2026-30792	A vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android, WebClient (Strategy sync, HTTP API client, config options engine modules) allows Application API Message Manipulation via Man-in-the-Middle. This vulnerability is associated with program files src/hbbs_http/sync.Rs, hbb_common/src/config.Rs and program routines Strategy merge loop in sync.Rs, Config::set_options(). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-3233	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-25070	XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain an OS command injection vulnerability in the /goform/PingTestSet endpoint that allows unauthenticated remote attackers to execute arbitrary operating system commands. Attackers can inject malicious commands through the destIp parameter to achieve remote code execution with root privileges on the network switch.	N/A	More Details
CVE-2026-25071	XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain a missing authentication vulnerability in the /switch_config.src endpoint that allows unauthenticated remote attackers to download device configuration files. Attackers can access this endpoint without credentials to retrieve sensitive configuration information including VLAN settings and IP addressing details.	N/A	More Details
CVE-2026-30841	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.6.2, passwordreset.php outputs $_GET["token"] and $_GET["email"] directly into HTML input value attributes using <?= $token ?> and <?= $email ?> without calling htmlspecialchars(). This allows reflected XSS by breaking out of the attribute context. This issue has been patched in version 4.6.2.	N/A	More Details
CVE-2026-30840	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.6.2, there is a server-side request forgery vulnerability in notification testers. This issue has been patched in version 4.6.2.	N/A	More Details
CVE-2026-30839	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.6.2, testwebhooknotifications.php does not validate the target URL against private/reserved IP ranges, enabling full-read SSRF. The server response is returned to the caller. This issue has been patched in version 4.6.2.	N/A	More Details
CVE-2026-30830	Defuddle cleans up HTML pages. Prior to version 0.9.0, the _findContentBySchemaText method in src/defuddle.ts interpolates image src and alt attributes directly into an HTML string without escaping. An attacker can use a " in the alt attribute to break out of the attribute context and inject event handler. This issue has been patched in version 0.9.0.	N/A	More Details
CVE-2026-30828	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.6.2, the url parameter can be used to retrieve local system files. This issue has been patched in version 4.6.2.	N/A	More Details
CVE-2026-30783	A vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android, WebClient (Client signaling, API sync loop, config management modules) allows Privilege Abuse. This vulnerability is associated with program files src/rendezvous_mediator.Rs, src/hbbs_http/sync.Rs and program routines API sync loop, api-server config handling. This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30824	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, the NVIDIA NIM router (/api/v1/nvidia-nim/*) is whitelisted in the global authentication middleware, allowing unauthenticated access to privileged container management and token generation endpoints. This issue has been patched in version 3.0.13.	N/A	More Details
CVE-2026-30823	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, there is an IDOR vulnerability, leading to account takeover and enterprise feature bypass via SSO configuration. This issue has been patched in version 3.0.13.	N/A	More Details
CVE-2026-30784	Missing Authorization, Missing Authentication for Critical Function vulnerability in rustdesk-server RustDesk Server rustdesk-server, rustdesk-server-pro on hbbs/hbbr on all server platforms (Rendezvous server (hbbs), relay server (hbbr) modules) allows Privilege Abuse. This vulnerability is associated with program files src/rendezvous_server.Rs, src/relay_server.Rs and program routines handle_punch_hole_request(), RegisterPeer handler, relay forwarding. This issue affects RustDesk Server: through 1.7.5, through 1.1.15.	N/A	More Details
CVE-2026-30822	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, unauthenticated users can inject arbitrary values into internal database fields when creating leads. This issue has been patched in version 3.0.13.	N/A	More Details

CVE-2026-30821	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, the /api/v1/attachments/:chatflowId/:chatId endpoint is listed in WHITELIST_URLS, allowing unauthenticated access to the file upload API. While the server validates uploads based on the MIME types defined in chatbotConfig.fullFileUpload.allowedUploadFileTypes, it implicitly trusts the client-provided Content-Type header (file.mimetype) without verifying the file's actual content (magic bytes) or extension (file.originalname). Consequently, an attacker can bypass this restriction by spoofing the Content-Type as a permitted type (e.g., application/pdf) while uploading malicious scripts or arbitrary files. Once uploaded via addArrayFilesToStorage, these files persist in backend storage (S3, GCS, or local disk). This vulnerability serves as a critical entry point that, when chained with other features like static hosting or file retrieval, can lead to Stored XSS, malicious file hosting, or Remote Code Execution (RCE). This issue has been patched in version 3.0.13.	N/A	More Details
CVE-2026-30820	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, Flowise trusts any HTTP client that sets the header x-request-from: internal, allowing an authenticated tenant session to bypass all /api/v1/** authorization checks. With only a browser cookie, a low-privilege tenant can invoke internal administration endpoints (API key management, credential stores, custom function execution, etc.), effectively escalating privilege. This issue has been patched in version 3.0.13.	N/A	More Details
CVE-2026-30785	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), Use of Password Hash With Insufficient Computational Effort vulnerability in rustdesk-client RustDesk Client rustdesk, hbb_common on Windows, MacOS, Linux (Password security module, config encryption, machine UID modules) allows Retrieve Embedded Sensitive Data. This vulnerability is associated with program files hbb_common/src/password_security.Rs, hbb_common/src/config.Rs, hbb_common/src/lib.Rs (get_uuid), machine-uid/src/lib.Rs and program routines symmetric_crypt(), encrypt_str_or_original(), decrypt_str_or_original(), get_uuid(), get_machine_id(). This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30789	Authentication Bypass by Capture-replay, Use of Password Hash With Insufficient Computational Effort vulnerability in rustdesk-client RustDesk Client rustdesk-client on Windows, MacOS, Linux, iOS, Android (Client login, peer authentication modules) allows Reusing Session IDs (aka Session Replay). This vulnerability is associated with program files src/client.Rs and program routines hash_password(), login proof construction. This issue affects RustDesk Client: through 1.4.5.	N/A	More Details
CVE-2026-30790	Improper Restriction of Excessive Authentication Attempts, Use of Password Hash With Insufficient Computational Effort vulnerability in rustdesk-server-pro RustDesk Server Pro rustdesk-server-pro on Windows, MacOS, Linux (Peer authentication, API login modules), rustdesk-server RustDesk Server (OSS) rustdesk-server on Windows, MacOS, Linux (Peer authentication, API login modules) allows Password Brute Forcing. This vulnerability is associated with program files src/server/connection.Rs and program routines Salt/challenge generation, SHA256(SHA256(pwd+salt)+challenge) verification. This issue affects RustDesk Server Pro: through 1.7.5; RustDesk Server (OSS): through 1.1.15.	N/A	More Details
CVE-2026-25073	XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain a stored cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary script content through the System Name field. Attackers can inject malicious scripts that execute in a victim's browser when the stored value is viewed due to improper output encoding.	N/A	More Details
CVE-2026-25072	XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain a predictable session identifier vulnerability in the /goform/SetLogin endpoint that allows remote attackers to hijack authenticated sessions. Attackers can predict session identifiers using insufficiently random cookie values and exploit exposed session parameters in URLs to gain unauthorized access to authenticated user sessions.	N/A	More Details
CVE-2026-26033	UPS Multi-UPS Management Console (MUMC) version 01.06.0001 (A03) contains an Unquoted Search Path or Element (CWE-428) vulnerability, which allows a user with write access to a directory on the system drive to execute arbitrary code with SYSTEM privileges.	N/A	More Details
CVE-2025-70042	An issue pertaining to CWE-918: Server-Side Request Forgery was discovered in oslabs-beta ThermaKube master.	N/A	More Details
CVE-2026-30941	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.14 and 9.5.2-alpha.1, NoSQL injection vulnerability allows an unauthenticated attacker to inject MongoDB query operators via the token field in the password reset and email verification resend endpoints. The token value is passed to database queries without type validation and can be used to extract password reset and email verification tokens. Any Parse Server deployment using MongoDB with email verification or password reset enabled is affected. When	N/A	More Details

	emailVerifyTokenReuseIfValid is configured, the email verification token can be fully extracted and used to verify a user's email address without inbox access. This vulnerability is fixed in 8.6.14 and 9.5.2-alpha.1.		
CVE-2026-1286	CWE-502: Deserialization of untrusted data vulnerability exists that could lead to loss of confidentiality, integrity and potential remote code execution on workstation when an admin authenticated user opens a malicious project file.	N/A	More Details
CVE-2026-28508	Idno is a social publishing platform. Prior to version 1.6.4, a logic error in the API authentication flow causes the CSRF protection on the URL unfurl service endpoint to be trivially bypassed by any unauthenticated remote attacker. Combined with the absence of a login requirement on the endpoint itself, this allows an attacker to force the server to make arbitrary outbound HTTP requests to any host, including internal network addresses and cloud instance metadata services, and retrieve the response content. This issue has been patched in version 1.6.4.	N/A	More Details
CVE-2025-11792	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 41124.	N/A	More Details
CVE-2025-11791	Sensitive information disclosure and manipulation due to insufficient authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, macOS, Windows) before build 41186, Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 41124.	N/A	More Details
CVE-2025-11790	Credentials are not deleted from Acronis Agent after plan revocation. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 41124.	N/A	More Details
CVE-2026-0847	A vulnerability in NLTK versions up to and including 3.9.2 allows arbitrary file read via path traversal in multiple CorpusReader classes, including WordListCorpusReader, TaggedCorpusReader, and BracketParseCorpusReader. These classes fail to properly sanitize or validate file paths, enabling attackers to traverse directories and access sensitive files on the server. This issue is particularly critical in scenarios where user-controlled file inputs are processed, such as in machine learning APIs, chatbots, or NLP pipelines. Exploitation of this vulnerability can lead to unauthorized access to sensitive files, including system files, SSH private keys, and API tokens, and may potentially escalate to remote code execution when combined with other vulnerabilities.	N/A	More Details
CVE-2026-23240	In the Linux kernel, the following vulnerability has been resolved: tls: Fix race condition in tls_sw_cancel_work_tx() This issue was discovered during a code audit. After cancel_delayed_work_sync() is called from tls_sk_proto_close(), tx_work_handler() can still be scheduled from paths such as the Delayed ACK handler or ksoftirqd. As a result, the tx_work_handler() worker may dereference a freed TLS object. The following is a simple race scenario: cpu0 cpu1 tls_sk_proto_close() tls_sw_cancel_work_tx() tls_write_space() tls_sw_write_space() if (!test_and_set_bit(BIT_TX_SCHEDULED, &tx_ctx->tx_bitmask)) set_bit(BIT_TX_SCHEDULED, &ctx->tx_bitmask); cancel_delayed_work_sync(&ctx->tx_work.work); schedule_delayed_work(&tx_ctx->tx_work.work, 0); To prevent this race condition, cancel_delayed_work_sync() is replaced with disable_delayed_work_sync().	N/A	More Details
CVE-2026-23239	In the Linux kernel, the following vulnerability has been resolved: espintcp: Fix race condition in espintcp_close() This issue was discovered during a code audit. After cancel_work_sync() is called from espintcp_close(), espintcp_tx_work() can still be scheduled from paths such as the Delayed ACK handler or ksoftirqd. As a result, the espintcp_tx_work() worker may dereference a freed espintcp ctx or sk. The following is a simple race scenario: cpu0 cpu1 espintcp_close() cancel_work_sync(&ctx->work); espintcp_write_space() schedule_work(&ctx->work); To prevent this race condition, cancel_work_sync() is replaced with disable_work_sync().	N/A	More Details
CVE-2026-28427	OpenDeck is Linux software for your Elgato Stream Deck. Prior to 2.8.1, the service listening on port 57118 serves static files for installed plugins but does not properly sanitize path components. By including ../ sequences in the request path, an attacker can traverse outside the intended directory and read any file OpenDeck can access. This vulnerability is fixed in 2.8.1.	N/A	More Details
CVE-2025-66024	The XWiki blog application allows users of the XWiki platform to create and manage blog posts. Versions prior to 9.15.7 are vulnerable to Stored Cross-Site Scripting (XSS) via the Blog Post Title. The vulnerability arises because the post title is injected directly into the HTML <title> tag without proper escaping. An attacker with permissions to create or edit blog posts can inject malicious JavaScript into the title field. This script will execute in the browser of any user (including administrators) who views the blog post. This leads to potential session hijacking or privilege escalation. The vulnerability has been patched in the blog application version 9.15.7 by adding missing escaping. No known workarounds are available.	N/A	More Details

CVE-2025-30413	Credentials are not deleted from Acronis Agent after plan revocation. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 40497, Acronis Cyber Protect 17 (Linux, macOS, Windows) before build 41186.	N/A	More Details
CVE-2026-29059	Windmill is an open-source developer platform for internal code: APIs, background jobs, workflows and UIs. Prior to version 1.603.3, an unauthenticated path traversal vulnerability exists in Windmill's get_log_file endpoint "(/api/w/{workspace}/jobs_u/get_log_file/{filename})". The filename parameter is concatenated into a file path without sanitization, allowing an attacker to read arbitrary files on the server using ../ sequences. This issue has been patched in version 1.603.3.	N/A	More Details
CVE-2026-25750	Langchain Helm Charts are Helm charts for deploying Langchain applications on Kubernetes. Prior to langchain-ai/helm version 0.12.71, a URL parameter injection vulnerability existed in LangSmith Studio that could allow unauthorized access to user accounts through stolen authentication tokens. The vulnerability affected both LangSmith Cloud and self-hosted deployments. Authenticated LangSmith users who clicked on a specially crafted malicious link would have their bearer token, user ID, and workspace ID transmitted to an attacker-controlled server. With this stolen token, an attacker could impersonate the victim and access any LangSmith resources or perform any actions the user was authorized to perform within their workspace. The attack required social engineering (phishing, malicious links in emails or chat applications) to convince users to click the crafted URL. The stolen tokens expired after 5 minutes, though repeated attacks against the same user were possible if they could be convinced to click malicious links multiple times. The fix in version 0.12.71 implements validation requiring user-defined allowed origins for the baseUrl parameter, preventing tokens from being sent to unauthorized servers. No known workarounds are available. Self-hosted customers must upgrade to the patched version.	N/A	More Details
CVE-2025-53706	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2025. Notes: none.	N/A	More Details
CVE-2025-13957	CWE-798: Use of Hard-coded Credentials vulnerability exists that could cause information disclosure and remote code execution when SOCKS Proxy is enabled, and administrator credentials and PostgreSQL database credentials are known. SOCKS Proxy is disabled by default.	N/A	More Details
CVE-2025-13902	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause condition where authenticated attackers can have a victim’s browser run arbitrary JavaScript when the victim hovers over a maliciously crafted element on a web server containing the injected payload.	N/A	More Details
CVE-2025-13901	CWE-404 Improper Resource Shutdown or Release vulnerability exists that could cause partial Denial of Service on Machine Expert protocol when an unauthenticated attacker sends malicious payload to occupy active communication channels.	N/A	More Details
CVE-2025-11739	CWE-502: Deserialization of Untrusted Data vulnerability exists that could cause arbitrary code execution with administrative privileges when a locally authenticated attacker sends a crafted data stream, triggering unsafe deserialization.	N/A	More Details
CVE-2022-4977	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-28507	Idno is a social publishing platform. Prior to version 1.6.4, there is a remote code execution vulnerability via chained import file write and template path traversal. This issue has been patched in version 1.6.4.	N/A	More Details
CVE-2026-28709	Unauthorized resource manipulation due to improper authorization checks. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2025-70046	An issue pertaining to CWE-829: Inclusion of Functionality from Untrusted Control Sphere was discovered in Miazzy oa-front-service master.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix out-of-bounds access in sysfs attribute read/write Some f2fs sysfs attributes suffer from out-of-bounds memory access and incorrect handling of integer values whose size is not 4 bytes. For example: vm:~# echo 65537 > /sys/fs/f2fs/vde/carve_out vm:~# cat /sys/fs/f2fs/vde/carve_out 65537 vm:~# echo 4294967297 > /sys/fs/f2fs/vde/atgc_age_threshold vm:~# cat /sys/fs/f2fs/vde/atgc_age_threshold 1 carve_out maps to {struct f2fs_sb_info}->carve_out, which is a 8-bit integer. However, the sysfs interface allows setting it to a value larger than 255, resulting in an out-of-range update. atgc_age_threshold maps to {struct		

2026-23235	atgc_management}->age_threshold, which is a 64-bit integer, but its sysfs interface cannot correctly set values larger than UINT_MAX. The root causes are: 1. __sbi_store() treats all default values as unsigned int, which prevents updating integers larger than 4 bytes and causes out-of-bounds writes for integers smaller than 4 bytes. 2. f2fs_sbi_show() also assumes all default values are unsigned int, leading to out-of-bounds reads and incorrect access to integers larger than 4 bytes. This patch introduces {struct f2fs_attr}->size to record the actual size of the integer associated with each sysfs attribute. With this information, sysfs read and write operations can correctly access and update values according to their real data size, avoiding memory corruption and truncation.	N/A	More Details
CVE-2026-30939	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.13 and 9.5.1-alpha.2, an unauthenticated attacker can crash the Parse Server process by calling a Cloud Function endpoint with a prototype property name as the function name. The server recurses infinitely, causing a call stack size error that terminates the process. Other prototype property names bypass Cloud Function dispatch validation and return HTTP 200 responses, even though no such Cloud Functions are defined. The same applies to dot-notation traversal. All Parse Server deployments that expose the Cloud Function endpoint are affected. This vulnerability is fixed in 8.6.13 and 9.5.1-alpha.2.	N/A	More Details
CVE-2026-30938	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.12 and 9.5.1-alpha.1, the requestKeywordDenylist security control can be bypassed by placing any nested object or array before a prohibited keyword in the request payload. This is caused by a logic bug that stops scanning sibling keys after encountering the first nested value. Any custom requestKeywordDenylist entries configured by the developer are equally by-passable using the same technique. All Parse Server deployments are affected. The requestKeywordDenylist is enabled by default. This vulnerability is fixed in 8.6.12 and 9.5.1-alpha.1. Use a Cloud Code beforeSave trigger to validate incoming data for prohibited keywords across all classes.	N/A	More Details
CVE-2026-23233	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid mapping wrong physical block for swapfile Xiaolong Guo reported a f2fs bug in bugzilla [1] [1] https://bugzilla.kernel.org/show_bug.cgi?id=220951 Quoted: "When using stress-ng's swap stress test on F2FS filesystem with kernel 6.6+, the system experiences data corruption leading to either: 1 dm-verity corruption errors and device reboot 2 F2FS node corruption errors and boot hangs The issue occurs specifically when: 1 Using F2FS filesystem (ext4 is unaffected) 2 Swapfile size is less than F2FS section size (2MB) 3 Swapfile has fragmented physical layout (multiple non-contiguous extents) 4 Kernel version is 6.6+ (6.1 is unaffected) The root cause is in check_swap_activate() function in fs/f2fs/data.c. When the first extent of a small swapfile (< 2MB) is not aligned to section boundaries, the function incorrectly treats it as the last extent, failing to map subsequent extents. This results in incorrect swap_extent creation where only the first extent is mapped, causing subsequent swap writes to overwrite wrong physical locations (other files' data). Steps to Reproduce 1 Setup a device with F2FS-formatted userdata partition 2 Compile stress-ng from https://github.com/ColinIanKing/stress-ng 3 Run swap stress test: (Android devices) adb shell "cd /data/stressng; ./stress-ng-64 --metrics-brief --timeout 60 --swap 0" Log: 1 Ftrace shows in kernel 6.6, only first extent is mapped during second f2fs_map_blocks call in check_swap_activate(): stress-ng-swap-8990: f2fs_map_blocks: ino=11002, file offset=0, start blkaddr=0x43143, len=0x1 (Only 4KB mapped, not the full swapfile) 2 in kernel 6.1, both extents are correctly mapped: stress-ng-swap-5966: f2fs_map_blocks: ino=28011, file offset=0, start blkaddr=0x13cd4, len=0x1 stress-ng-swap-5966: f2fs_map_blocks: ino=28011, file offset=1, start blkaddr=0x60c84b, len=0xff The problematic code is in check_swap_activate(): if ((pblock - SM_I(sbi)->main_blkaddr) % blks_per_sec || nr_pblocks % blks_per_sec || !f2fs_valid_pinned_area(sbi, pblock)) { bool last_extent = false; not_aligned++; nr_pblocks = roundup(nr_pblocks, blks_per_sec); if (cur_lblock + nr_pblocks > sis->max) nr_pblocks -= blks_per_sec; /* this extent is last one */ if (!nr_pblocks) { nr_pblocks = last_lblock - cur_lblock; last_extent = true; } ret = f2fs_migrate_blocks(inode, cur_lblock, nr_pblocks); if (ret) { if (ret == -ENOENT) ret = -EINVAL; goto out; } if (!last_extent) goto retry; } When the first extent is unaligned and roundup(nr_pblocks, blks_per_sec) exceeds sis->max, we subtract blks_per_sec resulting in nr_pblocks = 0. The code then incorrectly assumes this is the last extent, sets nr_pblocks = last_lblock - cur_lblock (entire swapfile), and performs migration. After migration, it doesn't retry mapping, so subsequent extents are never processed. " In order to fix this issue, we need to lookup block mapping info after we migrate all blocks in the tail of swapfile.	N/A	More Details
CVE-2026-23234	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid UAF in f2fs_write_end_io() As syzbot reported an use-after-free issue in f2fs_write_end_io(). It is caused by below race condition: loop device umount - worker_thread - loop_process_work - do_req_filebacked - lo_rw_aio - lo_rw_aio_complete - blk_mq_end_request - blk_update_request - f2fs_write_end_io - dec_page_count - folio_end_writeback - kill_f2fs_super - kill_block_super - f2fs_put_super : free(sbi) : get_pages(, F2FS_WB_CP_DATA) accessed sbi which is freed In kill_f2fs_super(), we will drop all page caches of f2fs inodes before call free(sbi), it guarantee that all folios should end its writeback, so it should be safe to access sbi before last folio_end_writeback(). Let's relocate ckpt thread wakeup flow	N/A	More Details

	before folio_end_writeback() to resolve this issue.		
CVE-2026-30930	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.1, The TimescaleDB export module constructs SQL queries using string concatenation with unsanitized system monitoring data. The normalize() method wraps string values in single quotes but does not escape embedded single quotes, making SQL injection trivial via attacker-controlled data such as process names, filesystem mount points, network interface names, or container names. This vulnerability is fixed in 4.5.1.	N/A	More Details
CVE-2026-30928	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.1, the /api/4/config REST API endpoint returns the entire parsed Glances configuration file (glances.conf) via self.config.as_dict() with no filtering of sensitive values. The configuration file contains credentials for all configured backend services including database passwords, API tokens, JWT signing keys, and SSL key passwords. This vulnerability is fixed in 4.5.1.	N/A	More Details
CVE-2026-2742	An authentication bypass vulnerability exists in Vaadin 14.0.0 through 14.14.0, 23.0.0 through 23.6.6, 24.0.0 through 24.9.7 and 25.0.0 through 25.0.1, applications using Spring Security due to inconsistent path pattern matching of reserved framework paths. Accessing the /VAADIN endpoint without a trailing slash bypasses security filters, and allowing unauthenticated users to trigger framework initialization and create sessions without proper authorization. Users of affected versions using Spring Security should upgrade as follows: 14.0.0-14.14.0 upgrade to 14.14.1, 23.0.0-23.6.6 to 23.6.7, 24.0.0 - 24.9.7 to 24.9.8, and 25.0.0-25.0.1 upgrade to 25.0.2 or newer. Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 14, 23, 24, 25 version.	N/A	More Details
CVE-2026-2741	Specially crafted ZIP archives can escape the intended extraction directory during Node.js download and extraction in Vaadin 14.2.0 through 14.14.0, 23.0.0 through 23.6.6, 24.0.0 through 24.9.8, and 25.0.0 through 25.0.2. Vaadin’s build process can automatically download and extract Node.js if it is not installed locally. If an attacker can intercept or control this download via DNS hijacking, a MITM attack, a compromised mirror, or a supply chain attack, they can serve a malicious archive containing path traversal sequences that write files outside the intended extraction directory. Users of affected versions should use a globally preinstalled Node.js version compatible with their Vaadin version, or upgrade as follows: 14.2.0-14.14.0 to 14.14.1, 23.0.0-23.6.6 to 23.6.7, 24.0.0-24.9.8 to 24.9.9, and 25.0.0-25.0.2 to 25.0.3 or newer. Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 14, 23, 24, 25 version.	N/A	More Details
CVE-2026-23236	In the Linux kernel, the following vulnerability has been resolved: fbdev: smscufx: properly copy ioctl memory to kernelspace The UFX_IOCTL_REPORT_DAMAGE ioctl does not properly copy data from userspace to kernelspace, and instead directly references the memory, which can cause problems if invalid data is passed from userspace. Fix this all up by correctly copying the memory before accessing it within the kernel.	N/A	More Details
CVE-2026-28710	Sensitive information disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.	N/A	More Details
CVE-2026-2273	CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exist that could cause execution of untrusted commands on the engineering workstation which could result in a limited compromise of the workstation and a potential loss of Confidentiality, Integrity and Availability of the subsequent system when an authenticated user opens a malicious project file.	N/A	More Details
CVE-2026-23237	In the Linux kernel, the following vulnerability has been resolved: platform/x86: classmate-laptop: Add missing NULL pointer checks In a few places in the Classmate laptop driver, code using the accel object may run before that object's address is stored in the driver data of the input device using it. For example, cmpc_accel_sensitivity_store_v4() is the "show" method of cmpc_accel_sensitivity_attr_v4 which is added in cmpc_accel_add_v4(), before calling dev_set_drvdata() for inputdev->dev. If the sysfs attribute is accessed prematurely, the dev_get_drvdata(&inputdev->dev) call in in cmpc_accel_sensitivity_store_v4() returns NULL which leads to a NULL pointer dereference going forward. Moreover, sysfs attributes using the input device are added before initializing that device by cmpc_add_acpi_notify_device() and if one of them is accessed before running that function, a NULL pointer dereference will occur. For example, cmpc_accel_sensitivity_attr_v4 is added before calling cmpc_add_acpi_notify_device() and if it is read prematurely, the dev_get_drvdata(&acpi->dev) call in cmpc_accel_sensitivity_show_v4() returns NULL which leads to a NULL pointer dereference going forward. Fix this by adding NULL pointer checks in all of the relevant places.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: romfs: check sb_set_blocksize() return value romfs_fill_super() ignores the return value of sb_set_blocksize(), which can fail if the requested block size is incompatible with the block device's configuration. This can be triggered by setting a loop device's block size larger than PAGE_SIZE using ioctl(LOOP_SET_BLOCK_SIZE, 32768),		

CVE-2026-23238	then mounting a romfs filesystem on that device. When sb_set_blocksize(sb, ROMBSIZE) is called with ROMBSIZE=4096 but the device has logical_block_size=32768, bdev_validate_blocksize() fails because the requested size is smaller than the device's logical block size. sb_set_blocksize() returns 0 (failure), but romfs ignores this and continues mounting. The superblock's block size remains at the device's logical block size (32768). Later, when sb_bread() attempts I/O with this oversized block size, it triggers a kernel BUG in folio_set_bh(): kernel BUG at fs/buffer.c:1582! BUG_ON(size > PAGE_SIZE); Fix by checking the return value of sb_set_blocksize() and failing the mount with -EINVAL if it returns 0.	N/A	More Details
CVE-2026-28497	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. Prior to version 2.03, an integer overflow vulnerability in the string-to-integer conversion routine (_Val) allows an unauthenticated remote attacker to bypass Content-Length restrictions and perform HTTP Request Smuggling. This can lead to unauthorized access, security filter bypass, and potential cache poisoning. The impact is critical for servers using persistent connections (Keep-Alive). This issue has been patched in version 2.03.	N/A	More Details
CVE-2026-28502	WWBN AVideo is an open source video platform. Prior to version 24.0, an authenticated Remote Code Execution (RCE) vulnerability was identified in AVideo related to the plugin upload/import functionality. The issue allowed an authenticated administrator to upload a specially crafted ZIP archive containing executable server-side files. Due to insufficient validation of extracted file contents, the archive was extracted directly into a web-accessible plugin directory, allowing arbitrary PHP code execution. This issue has been patched in version 24.0.	N/A	More Details
CVE-2026-28712	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect 17 (Windows) before build 41186.	N/A	More Details
CVE-2026-29046	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. Prior to version 2.04, TinyWeb accepts request header values and later maps them into CGI environment variables (HTTP_*). The parser did not strictly reject dangerous control characters in header lines and header values, including CR, LF, and NUL, and did not consistently defend against encoded forms such as %0d, %0a, and %00. This can enable header value confusion across parser boundaries and may create unsafe data in the CGI execution context. This issue has been patched in version 2.04.	N/A	More Details
CVE-2026-28711	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect 17 (Windows) before build 41186.	N/A	More Details
CVE-2026-30927	Admidio is an open-source user management solution. Prior to 5.0.6, in modules/events/events_function.php, the event participation logic allows any user who can participate in an event to register OTHER users by manipulating the user_uuid GET parameter. The condition uses || (OR), meaning if possibleToParticipate() returns true (event is open for participation), ANY user - not just leaders - can specify a different user_uuid and register/cancel participation for that user. The code then operates on $user->getValue('usr_id') (the target user from user_uuid) rather than the current user. This vulnerability is fixed in 5.0.6.	N/A	More Details
CVE-2026-30925	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.0-alpha.14 and 8.6.11, a malicious client can subscribe to a LiveQuery with a crafted $regex pattern that causes catastrophic backtracking, blocking the Node.js event loop. This makes the entire Parse Server unresponsive, affecting all clients. Any Parse Server deployment with LiveQuery enabled is affected. The attacker only needs the application ID and JavaScript key, both of which are public in client-side apps. This only affects LiveQuery subscription matching, which evaluates regex in JavaScript on the Node.js event loop. Normal REST and GraphQL queries are not affected because their regex is evaluated by the database engine. This vulnerability is fixed in 9.5.0-alpha.14 and 8.6.11.	N/A	More Details
CVE-2026-26002	Open OnDemand is an open-source high-performance computing portal. The Files application in OnDemand versions prior to 4.0.9 and 4.1.3 is susceptible to malicious input when navigating to a directory. This has been patched in versions 4.0.9 and 4.1.3. Versions below this remain susceptible.	N/A	More Details
CVE-2025-70039	An issue pertaining to CWE-78: Improper Neutralization of Special Elements used in an OS Command was discovered in linagora Twake v2023.Q1.1223.	N/A	More Details
CVE-2026-0846	A vulnerability in the `filestring()` function of the `nltk.util` module in nltk version 3.9.2 allows arbitrary file read due to improper validation of input paths. The function directly opens files specified by user input without sanitization, enabling attackers to access sensitive system files by providing absolute paths or traversal paths. This vulnerability can be exploited locally or remotely, particularly in scenarios where the function is used in web APIs or other interfaces that accept user-supplied input.	N/A	More Details
CVE-			

2025-70031	An issue pertaining to CWE-352: Cross-Site Request Forgery was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4.	N/A	More Details
CVE-2025-70030	An issue pertaining to CWE-1333: Inefficient Regular Expression Complexity (4.19) was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4.	N/A	More Details
CVE-2025-68402	FreshRSS is a free, self-hostable RSS aggregator. From 57e1a37 - 00f2f04, the lengths of the nonce was changed from 40 chars to 64. password_verify() is currently being called with a constructed string (SHA-256 nonce + part of a bcrypt hash) instead of the raw user password. Due to bcrypt's 72-byte input truncation, this causes password verification to succeed even when the user enters an incorrect password. This vulnerability is fixed in 1.27.2-dev (476e57b). The issue was only present in the edge branch and never in a stable release.	N/A	More Details
CVE-2026-29122	International Data Casting (IDC) SFX2100 satellite receiver comes with the `/bin/date` utility installed with the setuid bit set. This configuration grants elevated privileges to any local user who can execute the binary. A local actor is able to use the GTFObins resource to preform privileged file reads as the root user on the local file system. This allows an actor to be able to read any root read-only files, such as the /etc/shadow file or other configuration/secrets carrier files.	N/A	More Details
CVE-2026-30140	An incorrect access control vulnerability exists in Tenda W15E V02.03.01.26_cn. An unauthenticated attacker can access the /cgi-bin/DownloadCfg/RouterCfm.jpg endpoint to download the configuration file containing plaintext administrator credentials, leading to sensitive information disclosure and potential remote administrative access.	N/A	More Details
CVE-2025-70032	An issue pertaining to CWE-601: URL Redirection to Untrusted Site was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4.	N/A	More Details
CVE-2026-29123	A SUID root-owned binary in /home/xd/terminal/XDTerminal in International Data Casting (IDC) SFX2100 on Linux allows a local actor to potentially preform local privilege escalation depending on conditions of the system via execution of the affected SUID binary. This can be via PATH hijacking, symlink abuse or shared object hijacking.	N/A	More Details
CVE-2025-70038	An issue pertaining to CWE-79: Improper Neutralization of Input During Web Page Generation was discovered in linagora Twake v2023.Q1.1223. This allows attackers to execute arbitrary code.	N/A	More Details
CVE-2026-30917	Bucket is a MediaWiki extension to store and retrieve structured data on articles. Prior to 2.1.1, a stored XSS can be inserted into any Bucket table field that has a PAGE type, which will execute whenever a user views that table's corresponding Bucket namespace page. This vulnerability is fixed in 2.1.1.	N/A	More Details
CVE-2025-70034	An issue pertaining to CWE-1333: Inefficient Regular Expression Complexity (4.19) was discovered in mscdex ssh2 v1.17.0.	N/A	More Details
CVE-2025-70037	An issue pertaining to CWE-601: URL Redirection to Untrusted Site was discovered in linagora Twake v2023.Q1.1223. This allows attackers to obtain sensitive information and execute arbitrary code.	N/A	More Details
CVE-2025-15568	A command injection vulnerability was identified in the web module of Archer AXE75 v1.6/v1.0 router. An authenticated attacker with adjacent-network access may be able to perform remote code execution (RCE) when the router is configured with sysmode=ap. Successful exploitation results in root-level privileges and impacts confidentiality, integrity and availability of the device. This issue affects Archer AXE75 v1.6/v1.0: through 1.3.2 Build 20250107.	N/A	More Details
CVE-2026-29124	Multiple SUID root-owned binaries are found in /home/monitor/terminal, /home/monitor/kore-terminal, /home/monitor/IDE-DPack/terminal-dpack, and /home/monitor/IDE-DPack/terminal-dpack2 in International Data Casting (IDC) SFX2100 Satellite Receiver, which may lead to local privlidge escalation from the `monitor` user to root	N/A	More Details
CVE-2026-29125	IDC SFX2100 Satalite Recievers set the `/etc/resolv.conf` file to be world-writable by any local user, allowing DNS resolver tampering that can redirect network communications, facilitate man-in-the-middle attacks, and cause denial of service.	N/A	More Details
CVE-2025-70050	An issue pertaining to CWE-312: Cleartext Storage of Sensitive Information was discovered in lesspass lesspass v9.6.9 which allows attackers to obtain sensitive information.	N/A	More Details

CVE-2025-70048	An issue pertaining to CWE-319: Cleartext Transmission of Sensitive Information was discovered in Nexusoft NexusInterface v3.2.0-beta.2.	N/A	More Details
CVE-2026-29126	Incorrect permission assignment (world-writable file) in /etc/udhcpc/default.script in International Data Casting (IDC) SFX2100 Satellite Receiver allows a local unprivileged attacker to potentially execute arbitrary commands with root privileges (local privilege escalation and persistence) via modification of a root-owned, world-writable BusyBox udhcpc DHCP event script, which is executed when a DHCP lease is obtained, renewed, or lost.	N/A	More Details
CVE-2026-25041	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.23.22 and earlier, the PostgreSQL integration constructs shell commands using user-controlled configuration values (database name, host, password, etc.) without proper sanitization. The password and other connection parameters are directly interpolated into a shell command. This affects packages/server/src/integrations/postgres.ts.	N/A	More Details
CVE-2025-70028	An issue pertaining to CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') was discovered in Sunbird-Ed SunbirdEd-portal v1.13.4.	N/A	More Details
CVE-2026-25045	Budibase is a low code platform for creating internal tools, workflows, and admin panels. This issue is a combination of Vertical Privilege Escalation and IDOR (Insecure Direct Object Reference) due to missing server-side RBAC checks in the /api/global/users endpoints. A Creator-level user, who should have no permissions to manage users or organizational roles, can instead promote an App Viewer to Tenant Admin, demote a Tenant Admin to App Viewer, or modify the Owner's account details and all orders (e.g., change name). This is because the API accepts these actions without validating the requesting role, a Creator can replay Owner-only requests using their own session tokens. This leads to full tenant compromise.	N/A	More Details
CVE-2026-29121	International Data Casting (IDC) SFX2100 satellite receiver comes with the `/sbin/ip` utility installed with the setuid bit set. This configuration grants elevated privileges to any local user who can execute the binary. A local actor is able to use the GTFObins resource to preform privileged file reads as the root user on the local file system and may potentially lead to other avenues for preforming privileged actions.	N/A	More Details
CVE-2026-30916	Shescape is a simple shell escape library for JavaScript. Prior to 2.1.9, an attacker may be able to bypass escaping for the shell being used. This can result, for example, in exposure of sensitive information. This impacts users of Shescape that configure their shell to point to a file on disk that is a link to a link. The precise result of being affected depends on the actual shell used and incorrect shell identified by Shescape. This vulnerability is fixed in 2.1.9.	N/A	More Details
CVE-2026-30885	WWBN AVideo is an open source video platform. Prior to 25.0, the /objects/playlistsFromUser.json.php endpoint returns all playlists for any user without requiring authentication or authorization. An unauthenticated attacker can enumerate user IDs and retrieve playlist information including playlist names, video IDs, and playlist status for any user on the platform. This vulnerability is fixed in 25.0.	N/A	More Details
CVE-2026-23925	An authenticated Zabbix user (User role) with template/host write permissions is able to create objects via the configuration.import API. This can lead to confidentiality loss by creating unauthorized hosts. Note that the User role is normally not sufficient to create and edit templates/hosts even with write permissions.	N/A	More Details
CVE-2026-28484	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-1468	QuickCMS is vulnerable to Cross-Site Request Forgery across multiple endpoints. An attacker can craft special website, which when visited by the victim, will automatically send a POST request with victim's privileges. This software does not implement any protection against this type of attack. All forms available in this software are potentially vulnerable. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-28267	Multiple i-フィルター products are configured with improper file access permission settings. Files may be created or overwritten in the system directory or backup directory by a non-administrative user.	N/A	More Details
CVE-2026-	The import hook in CPython that handles legacy *.pyc files (SourcelessFileLoader) is incorrectly handled in FileLoader (a base class) and so does not use io.open_code() to read the .pyc files. sys.audit	N/A	More Details

2297	handlers for this audit event therefore do not fire.		
CVE-2026-30847	Wekan is an open source kanban tool built with Meteor. In versions 8.31.0 through 8.33, the notificationUsers publication in Wekan publishes user documents with no field filtering, causing the ReactiveCache.getUsers() call to return all fields including highly sensitive data such as bcrypt password hashes, active session login tokens, email verification tokens, full email addresses, and any stored OAuth tokens. Unlike Meteor's default auto-publication which strips the services field for security, custom publications return whatever fields the cursor contains, meaning all subscribers receive the complete user documents. Any authenticated user who triggers this publication can harvest credentials and active session tokens for other users, enabling password cracking, session hijacking, and full account takeover. This issue has been fixed in version 8.34.	N/A	More Details
CVE-2026-31802	node-tar is a full-featured Tar for Node.js. Prior to version 7.5.11, tar (npm) can be tricked into creating a symlink that points outside the extraction directory by using a drive-relative symlink target such as C:../../../target.txt, which enables file overwrite outside cwd during normal tar.x() extraction. This vulnerability is fixed in 7.5.11.	N/A	More Details
CVE-2026-22052	ONTAP versions 9.12.1 and higher with S3 NAS buckets are susceptible to an information disclosure vulnerability. Successful exploit could allow an authenticated attacker to view a listing of the contents in a directory for which they lack permission.	N/A	More Details
CVE-2026-2833	An HTTP request smuggling vulnerability (CWE-444) was found in Pingora's handling of HTTP/1.1 connection upgrades. The issue occurs when a Pingora proxy reads a request containing an Upgrade header, causing the proxy to pass through the rest of the bytes on the connection to a backend before the backend has accepted the upgrade. An attacker can thus directly forward a malicious payload after a request with an Upgrade header to that backend in a way that may be interpreted as a subsequent request header, bypassing proxy-level security controls and enabling cross-user session hijacking. Impact This vulnerability primarily affects standalone Pingora deployments where a Pingora proxy is exposed to external traffic. An attacker could exploit this to: * Bypass proxy-level ACL controls and WAF logic * Poison caches and upstream connections, causing subsequent requests from legitimate users to receive responses intended for smuggled requests * Perform cross-user attacks by hijacking sessions or smuggling requests that appear to originate from the trusted proxy IP Cloudflare's CDN infrastructure was not affected by this vulnerability, as ingress proxies in the CDN stack maintain proper HTTP parsing boundaries and do not prematurely switch to upgraded connection forwarding mode. Mitigation: Pingora users should upgrade to Pingora v0.8.0 or higher As a workaround, users may return an error on requests with the Upgrade header present in their request filter logic in order to stop processing bytes beyond the request header and disable downstream connection reuse.	N/A	More Details
CVE-2026-2835	An HTTP Request Smuggling vulnerability (CWE-444) has been found in Pingora's parsing of HTTP/1.0 and Transfer-Encoding requests. The issue occurs due to improperly allowing HTTP/1.0 request bodies to be close-delimited and incorrect handling of multiple Transfer-Encoding values, allowing attackers to send HTTP/1.0 requests in a way that would desync Pingora’s request framing from backend servers’. Impact This vulnerability primarily affects standalone Pingora deployments in front of certain backends that accept HTTP/1.0 requests. An attacker could craft a malicious payload following this request that Pingora forwards to the backend in order to: * Bypass proxy-level ACL controls and WAF logic * Poison caches and upstream connections, causing subsequent requests from legitimate users to receive responses intended for smuggled requests * Perform cross-user attacks by hijacking sessions or smuggling requests that appear to originate from the trusted proxy IP Cloudflare's CDN infrastructure was not affected by this vulnerability, as its ingress proxy layers forwarded HTTP/1.1 requests only, rejected ambiguous framing such as invalid Content-Length values, and forwarded a single Transfer-Encoding: chunked header for chunked requests. Mitigation: Pingora users should upgrade to Pingora v0.8.0 or higher that fixes this issue by correctly parsing message length headers per RFC 9112 and strictly adhering to more RFC guidelines, including that HTTP request bodies are never close-delimited. As a workaround, users can reject certain requests with an error in the request filter logic in order to stop processing bytes on the connection and disable downstream connection reuse. The user should reject any non-HTTP/1.1 request, or a request that has invalid Content-Length, multiple Transfer-Encoding headers, or Transfer-Encoding header that is not an exact “chunked” string match.	N/A	More Details
CVE-2026-28433	Misskey is an open source, federated social media platform. All Misskey servers running versions 10.93.0 and later, but prior to 2026.3.1, contain a vulnerability that allows importing other users' data due to lack of ownership validation. The impact of this vulnerability is estimated to be relatively low, as bad actors would require the ID corresponding to the target file for import. This vulnerability is fixed in 2026.3.1.	N/A	More Details
CVE-2026-28432	Misskey is an open source, federated social media platform. All Misskey servers prior to 2026.3.1 contain a vulnerability that allows bypassing HTTP signature verification. Although this is a vulnerability related to federation, it affects all servers regardless of whether federation is enabled or disabled. This vulnerability is fixed in 2026.3.1.	N/A	More Details

CVE-2026-28431	Misskey is an open source, federated social media platform. All Misskey servers running versions 8.45.0 and later, but prior to 2026.3.1, contain a vulnerability that allows bad actors access to data that they ordinarily wouldn't be able to access due to insufficient permission checks and proper input validation. This vulnerability occurs regardless of whether federation is enabled or not. This vulnerability could lead to a significant data breach. This vulnerability is fixed in 2026.3.1.	N/A	More Details
CVE-2026-1776	Camaleon CMS versions 2.4.5.0 through 2.9.0, prior to commit f54a77e, contain a path traversal vulnerability in the AWS S3 uploader implementation that allows authenticated users to read arbitrary files from the web server’s filesystem. The issue occurs in the download_private_file functionality when the application is configured to use the CamaleonCmsAwsUploader backend. Unlike the local uploader implementation, the AWS uploader does not validate file paths with valid_folder_path?, allowing directory traversal sequences to be supplied via the file parameter. As a result, any authenticated user, including low-privileged registered users, can access sensitive files such as /etc/passwd. This issue represents a bypass of the incomplete fix for CVE-2024-46987 and affects deployments using the AWS S3 storage backend.	N/A	More Details
CVE-2026-2836	A cache poisoning vulnerability has been found in the Pingora HTTP proxy framework’s default cache key construction. The issue occurs because the default HTTP cache key implementation generates cache keys using only the URI path, excluding critical factors such as the host header (authority). Operators relying on the default are vulnerable to cache poisoning, and cross-origin responses may be improperly served to users. Impact This vulnerability affects users of Pingora's alpha proxy caching feature who relied on the default CacheKey implementation. An attacker could exploit this for: * Cross-tenant data leakage: In multi-tenant deployments, poison the cache so that users from one tenant receive cached responses from another tenant * Cache poisoning attacks: Serve malicious content to legitimate users by poisoning shared cache entries Cloudflare's CDN infrastructure was not affected by this vulnerability, as Cloudflare's default cache key implementation uses multiple factors to prevent cache key poisoning and never made use of the previously provided default. Mitigation: We strongly recommend Pingora users to upgrade to Pingora v0.8.0 or higher, which removes the insecure default cache key implementation. Users must now explicitly implement their own callback that includes appropriate factors such as Host header, origin server HTTP scheme, and other attributes their cache should vary on. Pingora users on previous versions may also remove any of their default CacheKey usage and implement their own that should at minimum include the host header / authority and upstream peer’s HTTP scheme.	N/A	More Details
CVE-2026-28717	Local privilege escalation due to improper directory permissions. The following products are affected: Acronis Cyber Protect 17 (Windows) before build 41186.	N/A	More Details