

Security Bulletin 14 October 2026

Generated on 14 October 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-2026-42696	Improper Control of Generation of Code ('Code Injection') vulnerability in Royal Plugins SiteVault – Backup, Restore, Migration & Cloning sitevault-backup-restore-migration allows Remote Code Inclusion.This issue affects SiteVault – Backup, Restore, Migration & Cloning: from n/a through 1.5.19.	10.0	More Details
CVE-2026-108892	A vulnerability was determined in Linksys E1700 1.0.0.4.003. This vulnerability affects the function ssid1MACFilter of the file /goform/ssid1MACFilter of the component Mac Filter. This manipulation of the argument newap_text_%d causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-108804	A vulnerability was detected in TRENDnet TEW-751DR, TEW-752DRU and TEW733GR 1.03B01/1.03B03. Affected is the function fwrite of the file pigwidgeon.cgi of the component Web Management Backend. The manipulation of the argument service results in os command injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor confirms: "As this router was EOL'd in 2011, we have no way of testing if such vulnerability exists. We will notify our customers of a potential vulnerability on this product." This vulnerability only affects products that are no longer supported by the maintainer.	10.0	More Details
CVE-2026-102255	A Pre-authentication SSRF vulnerability exists in the SMA1000 Appliance Work Place interface due to an unintended alternate access path. By abusing this path, a remote unauthenticated attacker could potentially exploit this vulnerability to direct the appliance to issue requests on their behalf and reach internal functionality and perform unauthorized operations.	10.0	More Details
CVE-2026-108576	A vulnerability was found in TOZED X300 up to 6.01.3. This vulnerability affects the function process_ping of the component IPPingDiagnostics Handler. The manipulation of the argument Host results in os command injection. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2025-70518	The management portal's diagnostic ping tool of Fanvil x7a firmware version 2.6.0.1182 does not handle user supplied input securely. The lack of secure user input handling allows any unauthenticated attacker to inject commands and run code in the underlying Android operating system.	10.0	More Details
CVE-2026-94503	Unrestricted Upload of File with Dangerous Type vulnerability in PX-lab Zombify zombify allows Upload a Web Shell to a Web Server.This issue affects Zombify: from n/a through 1.7.7.	10.0	More Details

CVE-2026-76482	As part of Cisco's ongoing commitment to proactive security and product quality, the engineering team for Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76482 are related to issues with improper input verification that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-347.	10.0	More Details
CVE-2026-96207	Improper certificate validation in Microsoft Partner Center allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-108540	A flaw has been found in OpenSpug Spug up to 3.4.0/4.0.1. This impacts an unknown function of the file /exec/transfer of the component File Transfer. Executing a manipulation can lead to os command injection. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.9	More Details
CVE-2026-62024	Subscriber Arbitrary File Upload in CodeBard Help Desk <= 1.1.2 versions.	9.9	More Details
CVE-2026-106126	A command injection vulnerability in the Active Directory Events Listener of Tenable Identity Exposure (SaaS) allows an authenticated, low-privileged attacker to execute arbitrary commands as SYSTEM on the PDCe.	9.9	More Details
CVE-2026-62129	Contributor Arbitrary File Upload in Creator LMS <= 1.2.21 versions.	9.9	More Details
CVE-2026-94510	Authorization bypass through user-controlled key in Microsoft Bookings allows an unauthorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2026-108894	A security flaw has been discovered in Linksys E1700 1.0.0.4.003. Impacted is the function addStaticRoute of the file /goform/addStaticRoute of the component Static Route Handler. Performing a manipulation of the argument staticRoute_IP_setting/staticRoute_Netmask_setting/staticRoute_Gateway_setting/staticRoute_Metric_setting results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	9.9	More Details
CVE-2026-108893	A vulnerability was identified in Linksys E1700 up to 1.0.0.4.003. This issue affects the function setVlan of the file /goform/setVlan. Such manipulation of the argument vlan_set leads to stack-based buffer overflow. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.9	More Details
CVE-2026-108263	Astron Agent is an agentic workflow platform for building and running AI agents. Prior to 1.1.2, the default workflow code-node path through /console-api/workflow/code/run and /workflow/v1/run selects LocalExecutor in core/workflow/engine/nodes/code/code_node.py when CODE_EXEC_TYPE is not explicitly changed. LocalExecutor supplies complete Python builtins to dynamic code execution without the documented sandbox restrictions. An authenticated low-privilege tenant can execute code as root in the core-workflow container and use shared service and database credentials to bypass application-level tenant checks, read or modify other tenants' data, and disrupt shared services. This issue is fixed in version 1.1.2.	9.9	More Details
CVE-2026-108474	In JetBrains Exposed before 1.5.1 sQL injection was possible via unescaped string arguments of several SQL functions	9.8	More Details
CVE-2026-93943	Deserialization of Untrusted Data vulnerability in ThemeREX Group Convex convex allows Object Injection.This issue affects Convex: from n/a through 1.16.0.	9.8	More Details
CVE-2026-93937	Deserialization of Untrusted Data vulnerability in ThemeREX Group Hygia hygia allows Object Injection.This issue affects Hygia: from n/a through 1.21.0.	9.8	More Details
CVE-2026-93938	Deserialization of Untrusted Data vulnerability in ThemeREX Group Hogwords hogwords allows Object Injection.This issue affects Hogwords: from n/a through 1.2.7.	9.8	More Details
CVE-2026-93940	Deserialization of Untrusted Data vulnerability in ThemeREX Group Greeny greeny allows Object Injection.This issue affects Greeny: from n/a through 2.10.0.	9.8	More Details

CVE-2026-93941	Deserialization of Untrusted Data vulnerability in ThemeREX Group Edema edema allows Object Injection.This issue affects Edema: from n/a through 1.2.2.2.	9.8	More Details
CVE-2026-100730	A service console interface on openPDC and openHistorian deserializes a client-supplied data structure. On systems using Windows Authentication, an attacker must already be authenticated to reach this function; on systems without Windows Authentication, this is reachable by an unauthenticated network attacker. This allows an attacker to trigger deserialization of an arbitrary object graph, which could allow remote code execution under the privileges of the affected service account.	9.8	More Details
CVE-2026-93942	Deserialization of Untrusted Data vulnerability in ThemeREX Group Dwell dwell allows Object Injection.This issue affects Dwell: from n/a through 1.16.0.	9.8	More Details
CVE-2026-93945	Deserialization of Untrusted Data vulnerability in Axiomthemes Balance balance allows Object Injection.This issue affects Balance: from n/a through 1.12.0.	9.8	More Details
CVE-2026-93944	Deserialization of Untrusted Data vulnerability in ThemeREX Group Camelia camelia allows Object Injection.This issue affects Camelia: from n/a through 1.2.15.	9.8	More Details
CVE-2026-108551	openapi-typescript-codegen through 0.31.0 contains a code injection vulnerability that allows attackers controlling an OpenAPI document to inject JavaScript by supplying unescaped values interpolated into single-quoted string literals. Attackers can embed a single quote in path keys, parameter names, servers[0].url, or info.version to execute arbitrary JavaScript when generated clients are imported or service methods called.	9.8	More Details
CVE-2026-104398	Deserialization of Untrusted Data vulnerability in VillaTheme AFFI – Affiliate Marketing for WooCommerce affi-affiliate-marketing-for-woo allows Object Injection.This issue affects AFFI – Affiliate Marketing for WooCommerce: from n/a through 1.0.10.	9.8	More Details
CVE-2026-105892	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in rtCamp Inc. rtMedia for WordPress, BuddyPress and bbPress buddypress-media allows Path Traversal.This issue affects rtMedia for WordPress, BuddyPress and bbPress: from n/a through 4.7.13.	9.8	More Details
CVE-2026-106610	Incorrect Privilege Assignment vulnerability in miniOrange miniorange otp verification miniorange-otp-verification allows Privilege Escalation.This issue affects miniorange otp verification: from n/a through 5.5.7.	9.8	More Details
CVE-2026-108598	Floci 1.1.0 before 2.2.0 contains a code injection vulnerability in VtITemplateEngine that allows unauthenticated attackers to execute commands via unrestricted Velocity mapping templates. Attackers can create a REST API with a MOCK integration whose template uses \$util reflection to reach Runtime or ProcessBuilder, executing OS commands in the Floci JVM.	9.8	More Details
CVE-2026-39801	Subscriber Privilege Escalation in AIWU <= 1.5.9 versions.	9.8	More Details
CVE-2026-93936	Deserialization of Untrusted Data vulnerability in ThemeREX Group IPharm ipharm allows Object Injection.This issue affects IPharm: from n/a through 1.2.4.	9.8	More Details
CVE-2026-93935	Deserialization of Untrusted Data vulnerability in ThemeREX Group Let's Play playhockey allows Object Injection.This issue affects Let's Play: from n/a through 1.1.15.	9.8	More Details
CVE-2026-105278	The published Docker image for openPDC includes a fixed administrative credential with no forced change on first use. An attacker with network access to the management interface can authenticate using this credential and gain full administrative control of the application.	9.8	More Details
CVE-2026-93934	Deserialization of Untrusted Data vulnerability in ThemeREX Group Partiso partiso allows Object Injection.This issue affects Partiso: from n/a through 1.1.13.	9.8	More Details
CVE-2026-78835	Rocket Software Rocket Remote Desktop 18.0.8583.1 is vulnerable to Insufficiently Protected Credentials.	9.8	More Details
CVE-2026-15340	lwIP SMTP client does not check the size of inputs, potentially allowing a buffer overflow.	9.8	More Details
	The Advanced IP Blocker plugin for WordPress is vulnerable to Authentication Bypass in all versions up to,		

CVE-2026-104732	and including, 8.13.13 The vulnerability exists because `handle_login_action()` performs no server-side check — via transient, session marker, or equivalent — that a requester completed step-1 password authentication before processing a step-2 TOTP submission for the POSTed `user_id`; compounding this, an error branch in the function unconditionally mints a fresh `advaipbl-2fa-interim-{user_id}` nonce and delivers it in a `Location` header to any unauthenticated caller, after which `display_2fa_login_form_step_2()` renders a valid `advaipbl-2fa-verify-{user_id}` nonce in HTML — both nonces computed against a fixed `uid=0` empty-session context and therefore fully reusable by the attacker across subsequent requests. This makes it possible for unauthenticated attackers to bypass authentication entirely for any 2FA-enabled account, including administrators, by brute-forcing an unthrottled 6-digit TOTP code (no attempt counter, no account lockout, and no `wp_login_failed` firing) and receiving a fully authenticated session cookie via `wp_set_auth_cookie` without ever supplying the account password, resulting in complete site takeover. Exploitation requires only a known `user_id` for an account that has the plugin's 2FA feature enabled.	9.8	More Details
CVE-2026-94589	The Extensions For CF7 (Contact form 7 Database, Conditional Fields and Redirection) plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 3.4.5 via the extcf7_submit function. This is due to missing file extension, MIME type, and size validation in the signature field's validation_filter(), combined with the absence of PHP-execution guards in the upload directory and a sanitize_file_name() bypass that converts shell.php- into shell.php. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.	9.8	More Details
CVE-2026-103889	The 3D Product configurator for WooCommerce plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.16.2 via the 'xpv_image' parameter parameter. This is due to missing authentication and nonce checks on the wp_loaded handler combined with no sanitization of the xpv_image POST parameter before it is echoed unescaped into a Dompok-rendered HTML template with PHP execution enabled. This makes it possible for unauthenticated attackers to execute code on the server. The only nonce and authentication check in the handler is entirely enclosed in a block comment with no replacement, making the endpoint reachable via a single unauthenticated POST to any URL on the site.	9.8	More Details
CVE-2026-104803	The WPCOM Member plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.7.27 via the `uuid` and `code` parameters of the social-login callback handler registered on the `init` hook. The vulnerability exists because the `login` function's social-login flow performs no nonce validation, no OAuth state verification, and no per-visitor namespace isolation in the session store, allowing an unauthenticated attacker to issue a crafted GET request that writes an attacker-named, attacker-valued entry into the global session namespace (bypassing the per-visitor prefix by prepending an underscore), then issue a second GET request triggering `weapp_new_user()` to read that forged entry and resolve the attacker-supplied `openid` value to a bound WordPress account before `wp_set_auth_cookie()` establishes a fully authenticated session. This makes it possible for unauthenticated attackers to log in as any WordPress user — including administrators — whose bound social provider identifier (openid/unionid) is known or discoverable. Successful exploitation requires that the target site has at least one social provider configured (which activates the vulnerable handler) and that the attacker knows or can enumerate the victim account's bound openid or unionid.	9.8	More Details
CVE-2026-62045	Deserialization of Untrusted Data vulnerability in ThemeREX Group Booklovers booklovers allows Object Injection.This issue affects Booklovers: from n/a through 2.13.0.	9.8	More Details
CVE-2026-62046	Deserialization of Untrusted Data vulnerability in ThemeREX Group Gutentype gutentype allows Object Injection.This issue affects Gutentype: from n/a through 2.1.12.	9.8	More Details
CVE-2026-93674	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command.	9.8	More Details
CVE-2026-42716	Unauthenticated PHP Object Injection in Payever - WooCommerce Gateway <= 4.8.2 versions.	9.8	More Details
CVE-2026-93929	Deserialization of Untrusted Data vulnerability in ThemeREX Group Travesia travesia allows Object Injection.This issue affects Travesia: from n/a through 1.1.16.	9.8	More Details
CVE-2026-93930	Deserialization of Untrusted Data vulnerability in ThemeREX Group Tantra tantra allows Object Injection.This issue affects Tantra: from n/a through 2.9.0.	9.8	More Details
CVE-2026-93931	Deserialization of Untrusted Data vulnerability in ThemeREX Group Smash smash allows Object Injection.This issue affects Smash: from n/a through 1.12.0.	9.8	More Details

CVE-2026-93932	Deserialization of Untrusted Data vulnerability in ThemeREX Group Smart Casa smart-casa allows Object Injection.This issue affects Smart Casa: from n/a through 1.0.12.	9.8	More Details
CVE-2026-93933	Deserialization of Untrusted Data vulnerability in ThemeREX Group Rosalinda rosalinda allows Object Injection.This issue affects Rosalinda: from n/a through 1.2.4.	9.8	More Details
CVE-2026-93927	Deserialization of Untrusted Data vulnerability in Axiomthemes Veto veto allows Object Injection.This issue affects Veto: from n/a through 1.6.0.	9.8	More Details
CVE-2026-62032	Unauthenticated Local File Inclusion in DirectoryPress <= 3.6.27 versions.	9.8	More Details
CVE-2026-42718	Unauthenticated PHP Object Injection in Booster for WooCommerce <= 8.4.0 versions.	9.8	More Details
CVE-2026-108707	Wukong_HRM through commit 186115e contains an authentication bypass vulnerability in ParamAspect that allows unauthenticated attackers to call every HRM API endpoint by omitting the AUTH-TOKEN header. Attackers gain HR administrator access to read payslips, salary history and employee personal data, download attachments, and modify or delete company-wide HR records.	9.8	More Details
CVE-2026-66567	Unauthenticated PHP Object Injection in Anesta <= 1.5.3 versions.	9.8	More Details
CVE-2026-66568	Unauthenticated PHP Object Injection in Original <= 1.9.0 versions.	9.8	More Details
CVE-2026-66569	Unauthenticated PHP Object Injection in Kicker <= 2.2.1 versions.	9.8	More Details
CVE-2026-78529	Unauthenticated PHP Object Injection in Alliance <= 3.11 versions.	9.8	More Details
CVE-2026-78531	Unauthenticated PHP Object Injection in Jacqueline <= 2.22 versions.	9.8	More Details
CVE-2026-78533	Unauthenticated PHP Object Injection in Qwery <= 3.6.1 versions.	9.8	More Details
CVE-2026-78535	Unauthenticated PHP Object Injection in Photolia <= 1.0.3 versions.	9.8	More Details
CVE-2026-81797	Unauthenticated PHP Object Injection in Buzz Stone Magazine & Viral Blog WordPress Theme <= 1.0.2 versions.	9.8	More Details
CVE-2026-104028	The Anton Extensions WordPress plugin through 1.2.2 does not perform any capability check, nonce verification, or file-type validation before writing attacker-supplied content to an attacker-chosen path, allowing unauthenticated attackers to upload arbitrary PHP files and achieve remote code execution.	9.8	More Details
CVE-2026-66564	Unauthenticated PHP Object Injection in ShiftCV <= 3.0.14 versions.	9.8	More Details
CVE-2026-84251	The click5 CRM add-on to Ninja Forms WordPress plugin through 1.0.1 does not have authorisation and CSRF checks when updating options via a REST endpoint, and does not ensure that the option to be updated belongs to the click5 CRM add-on to Ninja Forms WordPress plugin through 1.0.1. As a result, unauthenticated attackers could change arbitrary blog options, allowing them to create a new administrator account and take over the site.	9.8	More Details
CVE-2026-	The click5 CRM add-on to WPForms WordPress plugin through 1.0.3 does not have authorisation and CSRF checks when updating options via a REST endpoint, and does not ensure that the option to be updated belongs to the click5 CRM add-on to WPForms WordPress plugin through 1.0.3. As a result, unauthenticated	9.8	More

84252	attackers could change arbitrary blog options, allowing them to create a new administrator account and take over the site.		Details
CVE-2026-84253	The click5 CRM add-on to Gravity Forms WordPress plugin through 1.0.3 does not have authorisation and CSRF checks when updating options via a REST endpoint, and does not ensure that the option to be updated belongs to the click5 CRM add-on to Gravity Forms WordPress plugin through 1.0.3. As a result, unauthenticated attackers could change arbitrary blog options, allowing them to create a new administrator account and take over the site.	9.8	More Details
CVE-2026-84254	The click5 CRM add-on to Contact Form 7 WordPress plugin through 1.0.4 does not have authorisation and CSRF checks when updating options via a REST endpoint, and does not ensure that the option to be updated belongs to the click5 CRM add-on to Contact Form 7 WordPress plugin through 1.0.4. As a result, unauthenticated attackers could change arbitrary blog options, allowing them to create a new administrator account and take over the site.	9.8	More Details
CVE-2026-84734	The Mindstien Quick Login WordPress plugin through 1.0 does not correctly validate a value supplied in the request against the visitor's own session before authenticating them, allowing unauthenticated attackers to obtain a session as the administrator account the Mindstien Quick Login WordPress plugin through 1.0 is configured with.	9.8	More Details
CVE-2026-84737	The Freeton WP WordPress plugin through 1.0.0 does not correctly validate the activation code when authenticating a user, allowing unauthenticated attackers to log in as any user whose email address they know, including administrators.	9.8	More Details
CVE-2026-85118	The AI Content Generator Marketing WordPress plugin through 1.0.0 does not enforce a nonce or capability check on some of its AJAX actions, allowing unauthenticated users to update and delete arbitrary WordPress options, which can be used to gain administrator access to the site.	9.8	More Details
CVE-2026-66086	In the modem OTA stack, there is a possible stack-based buffer overflow due to improper validation of scheduling information in SIB1 messages. This could lead to remote code execution or denial of service with no additional execution privileges needed.	9.8	More Details
CVE-2026-66565	Unauthenticated PHP Object Injection in FC United <= 1.1.1 versions.	9.8	More Details
CVE-2026-66563	Unauthenticated PHP Object Injection in Windsor <= 2.10 versions.	9.8	More Details
CVE-2026-42719	Subscriber PHP Object Injection in Dynamic User Directory <= 2.4 versions.	9.8	More Details
CVE-2026-62076	Unauthenticated PHP Object Injection in Kalles <= 1.1.7.1 versions.	9.8	More Details
CVE-2026-42723	Unauthenticated PHP Object Injection in CleanSkin <= 1.5.0 versions.	9.8	More Details
CVE-2026-62022	Unauthenticated Privilege Escalation in Tonda Membership <= 1.0.1 versions.	9.8	More Details
CVE-2026-85531	Improper verification of cryptographic signature vulnerability in Sipay Electronic Money and Payment Services Inc. OpenCart Virtual POS Module allows Signature Spoofing by Improper Validation. This issue affects OpenCart Virtual POS Module: from 26.8.2 before 26.9.1.	9.8	More Details
CVE-2026-62050	Unauthenticated PHP Object Injection in Splendour <= 1.23 versions.	9.8	More Details
CVE-2026-62051	Unauthenticated PHP Object Injection in Stargaze <= 1.10 versions.	9.8	More Details
CVE-2026-62052	Unauthenticated PHP Object Injection in Topsy <= 1.6 versions.	9.8	More Details
CVE-			More

2026-62053	Unauthenticated PHP Object Injection in Wine House <= 3.20 versions.	9.8	Details
CVE-2026-62054	Unauthenticated PHP Object Injection in Yacht Rental <= 2.6 versions.	9.8	More Details
CVE-2026-62077	Unauthenticated PHP Object Injection in Avala <= 1.1.4 versions.	9.8	More Details
CVE-2026-66483	Unauthenticated PHP Object Injection in Education Center <= 3.6.12 versions.	9.8	More Details
CVE-2026-62086	Unauthenticated PHP Object Injection in Juno <= 2.25 versions.	9.8	More Details
CVE-2026-62087	Unauthenticated PHP Object Injection in Equadio <= 1.1.4 versions.	9.8	More Details
CVE-2026-62090	Unauthenticated PHP Object Injection in WineShop <= 3.20 versions.	9.8	More Details
CVE-2026-62120	Unauthenticated PHP Object Injection in Law Office <= 3.20 versions.	9.8	More Details
CVE-2026-62123	Unauthenticated PHP Object Injection in Invetex <= 2.18 versions.	9.8	More Details
CVE-2026-62124	Unauthenticated PHP Object Injection in N7 Golf Club Sports & Events <= 2.21 versions.	9.8	More Details
CVE-2026-62125	Unauthenticated PHP Object Injection in Asia Garden <= 1.3.1 versions.	9.8	More Details
CVE-2026-66482	Unauthenticated PHP Object Injection in Drone Media <= 2.2.0 versions.	9.8	More Details
CVE-2026-86405	Improper verification of cryptographic signature vulnerability in Sipay Electronic Money and Payment Services Inc. PrestaShop Virtual POS Module allows Signature Spoofing by Improper Validation. This issue affects PrestaShop Virtual POS Module: from 26.8.1 before 26.9.1.	9.8	More Details
CVE-2026-104334	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote attacker to execute arbitrary code due to improper control of code generation.	9.8	More Details
CVE-2026-108107	PHPNuxBill through 2025.3.20 contains an unauthenticated SQL injection vulnerability in the radius.php FreeRADIUS REST endpoint that interpolates request parameters into whereRaw() queries. Attackers can send crafted username, macAddr or nasid parameters to the accounting or authenticate actions to extract customer records and credentials via time-based blind SQL injection.	9.8	More Details
CVE-2026-105110	OS Command Injection in the login.xgi CGI endpoint in Iskratel Innbox GPON ONT devices allows an unauthenticated remote attacker to execute arbitrary commands as root via the CLI parameter.	9.8	More Details
CVE-2026-107780	Dromara Skyeye through commit 003549ae5615bd114ba5bb8ddf6a8e8ead97c321 contains an OS command injection vulnerability in the unauthenticated /post/TtsController/textToSpeech endpoint via the format parameter. Attackers can inject a single quote into format to break out of the PowerShell string and execute commands as the Skyeye service account on Windows.	9.8	More Details
CVE-2026-107779	Dromara Skyeye through commit 003549ae5615bd114ba5bb8ddf6a8e8ead97c321 contains a missing authentication vulnerability in bundled xxl-job-admin JobInfoController endpoints annotated with @PermissionLimit(limit = false). Unauthenticated attackers can POST GLUE_SHELL, GLUE_PYTHON, or GLUE_POWERSHELL jobs with attacker-supplied glueSource to /jobinfo/addAndStart, executing commands on the executor host or stopping and deleting jobs.	9.8	More Details

CVE-2026-84272	IBM Guardium Data Protection 12.1 and 12.2.2 are vulnerable to missing authentication in the edge-controller component. An unauthenticated remote attacker could exploit this vulnerability to execute arbitrary container images and gain control of managed edge clusters.	9.8	More Details
CVE-2026-76500	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Application Policy Infrastructure Controller (APIC) engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76500 are related to issues with improper control of a resource through its lifetime that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-664.	9.8	More Details
CVE-2026-76501	A vulnerability in the Segment Routing over IPv6 (SRv6) Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM and SRv6 features are enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.	9.8	More Details
CVE-2026-104075	TVU Networks Receiver/Transceiver devices running firmware before version 7.9 contain an authentication bypass vulnerability in the web management login endpoint POST /tvu/Login that allows remote unauthenticated attackers to obtain an administrative session by submitting an empty or absent UserName parameter. Attackers can send a crafted HTTP request directly, bypassing client-side JavaScript validation, to receive a valid session cookie regardless of the password value and gain full administrative control of the device's web management interface.	9.8	More Details
CVE-2026-107704	The image_optimizer Ruby gem 1.3.0 through 1.9.0 contains an OS command injection vulnerability in ImageOptimizer#identify_format that allows attackers to execute commands by supplying a crafted image path when the identify option is enabled. Attackers controlling the path, such as an uploaded file name, can append shell metacharacters like ';' that are executed via Ruby backticks with the Ruby process privileges.	9.8	More Details
CVE-2026-107703	@enmaso/node-convert through 1.0.0 contains an OS command injection vulnerability in convert.js that allows attackers to execute shell commands via unsanitized filepath and convertTo arguments. Attackers can inject shell metacharacters or a single quote into the ImageMagick command run by child_process.exec() to execute operating system commands with Node.js process privileges.	9.8	More Details
CVE-2026-107700	dot-access 0.0.3 through 1.0.0 contains a code injection vulnerability that allows remote attackers to execute JavaScript by supplying crafted paths to get(). The path is concatenated into a new Function body in index.js, so attackers can reach constructor.constructor to load child_process and run operating system commands in the Node.js process.	9.8	More Details
CVE-2026-107699	ppt2png through 0.0.6 contains an OS command injection vulnerability that allows attackers to execute operating system commands by supplying unsanitized input or output path arguments. Attackers can append shell metacharacters such as ';' to file names passed to child_process.exec() in ppt2png.js, running commands with Node.js process privileges.	9.8	More Details
CVE-2026-95606	Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP The Events Calendar allows Object Injection. This issue affects The Events Calendar: from n/a through 6.17.4.	9.8	More Details
CVE-2026-76268	In Splunk Enterprise versions below 10.4.3 and 10.2.7, an unauthenticated user with network access to the Patroni Representational State Transfer (REST) Application Programming Interface (API) on a search head cluster member could execute attacker-controlled operating-system commands. The vulnerability is possible because this interface does not require authentication for critical configuration operations. For more information see Sidecar configuration settings (https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/10.2/splunk-sidecars/sidecar-configuration-settings) in the Splunk documentation. Splunk Enterprise versions 10.0.x and 9.4.x are not affected.	9.8	More Details
CVE-2026-9209	mJobTime through build 15.7.3.32 contains an unauthenticated SQL execution vulnerability in the Login.aspx admin panel handlers, where the runQueryButton postback and exportSqlQuery_Server PageMethod execute caller-supplied SQL against the backing Sybase SQL Anywhere database using DBA/sysadmin privileges with no server-side authentication enforced beyond a client-side sessionStorage flag. Attackers can submit arbitrary SQL through these exposed endpoints to invoke xp_cmdshell and xp_read_file, achieving pre-authentication remote code execution as LocalSystem via a single HTTP request.	9.8	More Details
CVE-2026-93034	SGLang contains an arbitrary code execution vulnerability caused by the ZMQ message decoder unconditionally deserializing PickleWrapper payloads via pickle.loads() in _maybe_unwrap_pickle without type allowlisting or authentication; this vulnerability persists via the msgpack path even when SGLANG_USE_PICKLE_IPC is disabled, and becomes remotely exploitable if data-parallel attention is enabled with a non-loopback --dist-init-addr setting.	9.8	More Details

CVE-2026-76284	Improper Neutralization. Splunk addressed multiple internally identified vulnerabilities in Splunk Enterprise versions 10.4.3, 10.2.7, 10.0.10, and 9.4.15. The vulnerabilities are grouped by Common Weakness Enumeration (CWE), with one Common Vulnerabilities and Exposures (CVE) identifier assigned to each group. See Details for more information.	9.8	More Details
CVE-2026-14992	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 vulnerable to buffer overflow.	9.8	More Details
CVE-2026-14502	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to obtain administrative access due to failure to reject empty passwords during LDAP authentication.	9.8	More Details
CVE-2026-14269	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. An unauthenticated remote attacker could overflow the buffer and execute arbitrary code on the system.	9.8	More Details
CVE-2026-76285	Improper Adherence to Coding Standards. Splunk addressed multiple internally identified vulnerabilities in Splunk Enterprise versions 10.4.3, 10.2.7, 10.0.10, and 9.4.15. The vulnerabilities are grouped by Common Weakness Enumeration (CWE), with one Common Vulnerabilities and Exposures (CVE) identifier assigned to each group. See Details for more information.	9.8	More Details
CVE-2026-15762	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.	9.8	More Details
CVE-2026-14991	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 is vulnerable to a buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	9.8	More Details
CVE-2026-87659	A critical authorization bypass vulnerability exists in the Management Server handling of Brocade Fabric OS versions before 10.0.1. A compromised switch connected to the fabric can transmit crafted inband Fibre Channel vendor-unique CT (Common Transport) management requests to bypass administrative authentication. Successful exploitation allows an unauthorized peer switch to execute administrative actions on the target device, including resetting administrative passwords, initiating system reboots, and triggering firmware downloads.	9.8	More Details
CVE-2026-103646	The Ultimate Multisite WordPress plugin before 2.17.0 does not require authentication before a logged-out checkout is linked to, and logged in as, an existing WordPress account matching the submitted email address, and its duplicate-account check normalizes that address differently from the lookup used to create the customer, so an unauthenticated attacker can log in as any existing user, including a Network Super Admin, whose email address they know. This bypass is not addressed by the 2.15.1 fix for CVE-2026-75957 and remains exploitable in all versions up to and including 2.16.1, the releases that fix was expected to cover. Exploitation requires a checkout form configured without a password field (auto-generated password) and a target account that has no existing customer record in the Ultimate Multisite WordPress plugin before 2.17.0.	9.8	More Details
CVE-2026-103692	The Frontend Dashboard WordPress plugin before 3.0.5 does not perform any authorisation or nonce check on actions available to unauthenticated users that call an attacker-chosen PHP function or class method with the request data, allowing unauthenticated users to take over any account, including administrators.	9.8	More Details
CVE-2026-107459	The SecuShare Pro developed by Openfind has an OS Command Injection vulnerability. Unauthenticated remote attackers can inject arbitrary OS commands and execute them on the server.	9.8	More Details
CVE-2026-16340	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write in the RFC2047 encoded-word parser.	9.8	More Details
CVE-2026-92555	Insertion of sensitive information into sent data vulnerability in AKIN Software Computer Import-Export Industry and Trade Co. Ltd. AKINSOFT WOLVOX Control Panel allows Pull Data from System Resources. This issue affects AKINSOFT WOLVOX Control Panel: from 26.02.25 before 26.02.26.	9.8	More Details
CVE-2026-76499	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Application Policy Infrastructure Controller (APIC) engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76499 are related to improper neutralization issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-707. 	9.8	More Details
CVE-	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Application Policy Infrastructure Controller (APIC) engineering team has conducted a comprehensive internal security		More

2026-76498	review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76498 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-284.	9.8	Details
CVE-2026-76486	A vulnerability in the VXLAN Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a Denial-of-Service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM feature is enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.	9.8	More Details
CVE-2026-76465	A vulnerability in the MPLS Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation when an affected device is processing an MPLS echo-request packet. An attacker could exploit this vulnerability by sending a crafted MPLS echo-request to an IP address on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes, which could result in a device reload and a DoS condition.	9.8	More Details
CVE-2026-105192	LMCache multiprocess mode, also called distributed mode, opens an unauthenticated ZeroMQ ROUTER so worker processes can register and share KV cache blocks. Messages on that socket are msgpack. Extension code 1 is passed to DeviceIPCWrapper.Deserialize, which calls pickle.loads, while the server is still decoding request arguments and before the handler runs. A single unauthenticated ZMQ DEALER message to the transport port (default 5555) therefore executes code as the user the LMCache process runs as. Official container images run that process as root. The transport binds to localhost unless the operator sets a routable address with --host, which is how multi-node deployments let peers connect.	9.8	More Details
CVE-2025-70521	The management portal's diagnostic ping tool of Fanvil x7a firmware version 2.6.0.1182 does not handle user supplied input securely. The lack of secure user input handling allows any unauthenticated attacker to inject commands and run code in the underlying Android operating system.	9.8	More Details
CVE-2026-107204	LMCache through 0.5.5 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute Python code by posting scripts to the /run_script endpoint. Attackers can recover real builtins through the injected FastAPI app object, bypassing the guarded __import__, to import os and run operating system commands as the LMCache process.	9.8	More Details
CVE-2026-107908	A heap-based out-of-bounds write in the BoltReadHandler function (src/bolt/bolt_api.c) in FalkorDB before 4.20.0 allows a remote unauthenticated attacker to cause a denial of service and possibly execute arbitrary code by sending a Bolt RESET message with an attacker-chosen chunk size to the Bolt port. The handler checks the size only with ASSERT(), which is compiled out in release builds, then computes a destination pointer from the wire-supplied 16-bit size and moves buffered data up to about 64 KiB backwards past the start of the read buffer. Only deployments that enable the Bolt endpoint (BOLT_PORT, disabled by default) are affected.	9.8	More Details
CVE-2026-62252	Homer is open source telecom observability software. Prior to version 11.0.283, on every fresh Homer deployment using internal authentication, the bootstrap process automatically creates an `admin` account with the password `sipcapture` (stored as a legacy SHA-256 hex hash). There is no first-login forced-change mechanism. Any attacker who reaches the login endpoint immediately gains full administrative access. Version 11.0.283 patches the issue.	9.8	More Details
CVE-2026-62253	Homer is open source telecom observability software. Prior to version 11.0.283, both JWT middleware functions (`JWTMiddleware` and `JWTMiddlewareV4`) immediately return `next(c)` when `jwtSecret == ""`. The JWT secret defaults to an empty string. On a default installation, all protected API endpoints under `/api/v1`, `/api/v3`, and `/api/v4` are completely unauthenticated. Version 11.0.283 patches the issue.	9.8	More Details
CVE-2026-76455	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76455 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-284.	9.8	More Details
CVE-2026-76459	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76459 are related to out-of-bounds write issues that are grouped under the Common Weakness Enumeration (CWE) CWE-787.	9.8	More Details
CVE-	A double free and use-after-free vulnerability in the RdbLoadDeletedNodes function of the RDB graph decoders (src/serializers/decoders*/decode_graph_entities.c) in FalkorDB before 4.18.1 allows a remote attacker who can issue Redis replication commands (for example, against an instance with no password		

2026-5759	configured) to cause a denial of service or execute arbitrary code in the redis-server process by supplying a crafted RDB stream whose deleted-nodes buffer length is not a multiple of sizeof(NodeID). The length check relies on ASSERT(), which is compiled out in release builds, so the function continues after freeing the buffer, reading it and freeing it a second time.	9.8	More Details
CVE-2026-88131	Deserialization of untrusted data in Microsoft Dataverse allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-78401	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote unauthenticated attacker to execute arbitrary code on the system due to the deserialization of untrusted data.	9.8	More Details
CVE-2026-85097	The Bricksforge plugin for WordPress is vulnerable to unauthenticated arbitrary file upload in versions up to, and including, 3.1.8.9. This is due to insufficient validation of the attacker-controlled URL field in the 'temporaryFileUploads' parameter during form submission. An unauthenticated attacker can first obtain a valid nonce via the bricksforge_regenerate_nonce AJAX endpoint, then upload a GIF/PHP polyglot file to the temporary upload directory where MIME type validation is correctly performed. Subsequently, the attacker can submit a form with a crafted 'temporaryFileUploads' parameter where the server-side file path points to the validated GIF file, but the attacker-controlled url field ends with a .php extension. This makes it possible for unauthenticated attackers to upload and execute arbitrary PHP code on the server.	9.8	More Details
CVE-2026-77900	Missing authentication for critical function in Azure App Service allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-84249	IBM Guardium Data Protection 12.2, and 12.2.2 could allow a remote attacker to execute arbitrary management operations due to missing authentication for critical function.	9.8	More Details
CVE-2026-78406	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote unauthenticated attacker to execute arbitrary code on the system due to the deserialization of untrusted data.	9.8	More Details
CVE-2026-76485	A vulnerability in the VXLAN Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a Denial-of-Service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM feature is enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.	9.8	More Details
CVE-2026-107722	fast-jwt provides fast JSON Web Token (JWT) implementation. From 6.2.0 until 6.3.0, fast-jwt can misclassify RSA public-key text as an HMAC secret when the key has non-whitespace content before its PEM header. In src/crypto.js, performDetectPublicKeyAlgorithms trims whitespace but publicKeyPemMatcher remains start-anchored, so comments, control characters, zero-width characters, or wrapper text can prevent PEM detection and reach the HMAC fallback. An attacker who knows the public key bytes can sign arbitrary HS256 claims with that public material when HS256 is inferred or allowed, resulting in authentication or authorization bypass. An asymmetric-only algorithm allowlist prevents the attack. This issue is fixed in version 6.3.0.	9.8	More Details
CVE-2026-80381	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute unauthorized SQL statements due to SQL injection.	9.8	More Details
CVE-2026-75875	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to path traversal.	9.8	More Details
CVE-2026-56857	On Windows, when the target of Root.Mkdir or Root.MkdirAll is a junction pointing to an empty location, the operation can create a directory at the junction target even when that target is located outside the root. This only applies to operations where the last path component is a junction (path/to/junction, but not path/junction/target).	9.8	More Details
CVE-2026-76480	As part of Cisco's ongoing commitment to proactive security and product quality, the engineering team for Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76480 are related to issues with improper authentication that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-306.	9.8	More Details
	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote		

CVE-2026-76471	attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation of data that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API of an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes, which could result in a reload of the device and a DoS condition.	9.8	More Details
CVE-2026-69435	Missing authorization in Azure SRE Agent allows an authorized attacker to elevate privileges over a network.	9.6	More Details
CVE-2026-76464	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by this CVE-2026-76464 are related to buffer management issues that are grouped under the Common Weakness Enumeration (CWE) CWE-119.	9.6	More Details
CVE-2026-107206	LMCache through 0.5.5 contains a missing authentication vulnerability in the multiprocess mode HTTP server that allows remote unauthenticated attackers to access management endpoints listening on all interfaces by default. Attackers can read environment credentials via GET /env and configuration via GET /config, clear caches, delete cache objects, and modify tenant quotas to evict other tenants' cached data.	9.4	More Details
CVE-2026-108753	Agnaistic agnai through 1.0.555 contains a hard-coded credentials vulnerability in self-host.docker-compose.yml, which sets a fixed admin password and public JWT secret. Unauthenticated attackers can log in as admin or sign their own JWT with admin: true to impersonate users, reset passwords, and change server configuration.	9.4	More Details
CVE-2026-93582	The HTTP Basic Authentication modules in ((OTRS)) Community Edition 6 and prior accept the authenticated username from either the REMOTE_USER or HTTP_REMOTE_USER environment variable. In CGI and mod_perl based deployments, HTTP request headers may be mapped to corresponding HTTP_* environment variables. As a result, an unauthenticated remote attacker can supply a crafted Remote-User request header which is exposed to the application as HTTP_REMOTE_USER. When HTTP Basic Authentication is configured as the authentication backend, OTRS trusts this value as an already authenticated username and does not perform an additional password verification. An attacker may therefore authenticate through the Generic Interface as an existing agent or customer user without knowing the corresponding credentials. The resulting privileges depend on the account being impersonated. Successful exploitation may allow access to confidential information and modification of data or configuration with the permissions of the affected user. Exploitation requires HTTP Basic Authentication to be configured as an authentication backend and a web server environment in which attacker-controlled HTTP headers are exposed through the corresponding HTTP_* environment variables. OTRS 7 and later are not affected by this attack vector due to the use of Mojolicious/Hypnotoad and does not expose arbitrary request headers through %ENV in the manner required for exploitation. The supported REMOTE_USER mechanism additionally requires validation through the configured SSO shared secret. The unused HTTP_REMOTE_USER fallback has nevertheless been removed as a security-hardening measure. Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	9.4	More Details
CVE-2026-95605	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Passionate Programmer Peter WP Data Access allows Blind SQL Injection. This issue affects WP Data Access: from n/a through 5.5.82.	9.3	More Details
CVE-2026-59346	VMware Workstation and Fusion contain an integer-overflow vulnerability. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Affected versions: - VMware Workstation: 25H2, 26H1 (fixed in 26H1u1) - VMware Fusion: 25H2, 26H1 (fixed in 26H1u1)	9.3	More Details
CVE-2026-96331	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdreams Ajax Search Pro ajax-search-pro allows Blind SQL Injection.This issue affects Ajax Search Pro: from n/a through 4.29.1.	9.3	More Details
CVE-2026-14990	IBM DataPower Gateway 10.6.0.0 through 10.6.0.10 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	9.3	More Details
CVE-2026-105889	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tickera Tickera tickera-event-ticketing-system allows Blind SQL Injection.This issue affects Tickera: from n/a through 3.6.0.6.	9.3	More Details
CVE-2026-108261	Tina is a headless content management system. Prior to tinacms 3.14.0 and @tinacms/app 2.5.14, the /~/* admin preview route in packages/tinacms/src/admin/index.tsx can turn an attacker-controlled hash-router splat into an off-origin iframe URL through packages/@tinacms/app/src/preview.tsx, while packages/@tinacms/app/src/lib/preview-origin.ts derives expectedOrigin from that same URL for the GraphQL message channel in packages/@tinacms/app/src/lib/graphql-reducer.ts. An unauthenticated attacker can send a crafted link to a signed-in editor, cause the admin to frame an attacker origin, and have	9.3	More Details

	that frame treated as the trusted preview. The attacker-controlled frame can submit GraphQL reads or mutations that the admin executes with the editor credentials, exposing or modifying protected content. This issue is fixed in tinacms 3.14.0 and @tinacms/app 2.5.14.		
CVE-2026-107935	A path traversal vulnerability was found in gvproxy, the network forwarder provided by the gvisor-tap-vsock package. The unauthenticated /services/forwarder/expose endpoint does not validate the caller-supplied socket path, allowing an attacker to delete arbitrary files on the host system.	9.3	More Details
CVE-2026-93947	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shinetheme Traveler traveler allows Blind SQL Injection.This issue affects Traveler: from n/a through 3.2.9.	9.3	More Details
CVE-2026-84244	IBM Guardium Data Protection 12.2 IBM Security Guardium Data Protection is vulnerable to stored cross-site scripting (XSS) in the Quick Search results grid. An unauthenticated attacker who can influence monitored database traffic could execute malicious script in the browser of an authenticated Guardium user.	9.3	More Details
CVE-2026-96327	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VibeThemes WPLMS wplms_plugin allows Blind SQL Injection.This issue affects WPLMS: from n/a before 1.9.9.8.2.	9.3	More Details
CVE-2026-107845	Contao is an Open Source CMS. From version 4.0.0 until 5.3.50 and 5.7.12, an unauthenticated visitor can submit a comment whose email or website metadata is rendered without sufficient attribute and URL encoding by listComments() in comments-bundle/contao/dca/tl_comments.php. When a backend user opens the Comments module, attacker-controlled script can execute in the Contao backend origin under that user's session. Unpublished comments remain visible to moderators, so moderation does not prevent exposure. This issue is fixed in versions 5.3.50 and 5.7.12.	9.3	More Details
CVE-2026-40800	Subscriber SQL Injection in ELEX WooCommerce Advanced Bulk Edit Products, Prices & Attributes <= 1.5.3 versions.	9.3	More Details
CVE-2026-96328	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in jegtheme JNews - Pay Writer jnews-pay-writer allows Blind SQL Injection.This issue affects JNews - Pay Writer: from n/a through 12.0.1.	9.3	More Details
CVE-2026-96809	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MultiNet Interactive AB EduAdmin Booking eduadmin-booking allows Blind SQL Injection.This issue affects EduAdmin Booking: from n/a before 6.0.0.	9.3	More Details
CVE-2026-62031	Unauthenticated SQL Injection in uListing <= 2.2.0 versions.	9.3	More Details
CVE-2026-96330	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in tagDiv tagDiv Opt-In Builder td-subscription allows Blind SQL Injection.This issue affects tagDiv Opt-In Builder: from n/a through 1.7.6.	9.3	More Details
CVE-2026-78357	Previously issued authentication tokens are not immediately invalidated when an OTRS agent or customer user account is deactivated or its password is changed. As a result, an existing JWT may remain valid until its regular expiration time, which can be approximately 16 hours. An attacker who has previously obtained a valid authentication token can therefore continue to access OTRS with the privileges of the affected agent or customer user even after the corresponding account has been deactivated or the user's password has been changed. The vulnerability does not allow an attacker to obtain authentication tokens by itself. Exploitation requires possession of a previously issued and still valid token. The actual impact depends on the privileges associated with the compromised token. Customer user tokens are limited to the permissions of the affected customer account, while agent tokens may provide access to broader ticket, customer, or administrative functionality depending on the assigned permissions. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X	9.1	More Details
CVE-2026-107202	A command injection vulnerability exists in the h-ui (version v0.0.25 and below) administrative API due to improper validation of the listen configuration field. When an authenticated administrator submits a value containing shell metacharacters, the application constructs nftables/iptables rule strings using fmt.Sprintf and executes them via bash -c as root. Because the listen field lacks port or format validation, arbitrary OS commands can be injected and executed with root privileges.	9.1	More Details
CVE-2026-20328	A vulnerability in the web-based management interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an unauthenticated, remote attacker to gain unauthorized access to an affected application. This vulnerability is due to improper checks during the password reset process. An attacker could exploit this vulnerability by sending a malicious request to the web-based management interface. A successful exploit could allow the attacker to reset the password of an arbitrary account, including high-privileged administrative user accounts, possibly allowing the attacker to gain unauthorized access to the application as any user.	9.1	More Details

CVE-2026-92414	: Session Fixation / Session Reuse across Users vulnerability in Apache Jackrabbit. Jackrabbit WebDAV server attaches a cached authenticated session on any Lock-Token/TransactionId/SubscriptionId/If-header field token match with no credential check. This issue affects Apache Jackrabbit: from 2.23.0 through 2.23.5, from 2.22.0 through 2.22.4, from 2.20.0 through 2.20.17. Users are recommended to upgrade to versions 2.23.6, 2.22.5, or 2.20.18 which fix the issue.	9.1	More Details
CVE-2026-107909	A heap-based out-of-bounds write in the ws_read_frame function (src/bolt/ws.c) and the buffer_apply_mask function (src/bolt/buffer.c) in FalkorDB before 4.20.0 allows a remote unauthenticated attacker to cause a denial of service and possibly corrupt heap memory by sending a WebSocket frame with a 64-bit extended payload length to the Bolt port. The payload length is not bounded, and the only bounds check in buffer_apply_mask is an ASSERT(), which is compiled out in release builds, so the function XORs memory beyond the end of the receive buffer with the attacker-supplied mask key. Only deployments that enable the Bolt endpoint (BOLT_PORT, disabled by default) are affected.	9.1	More Details
CVE-2026-108109	PHPNuxBill through 2025.3.20 contains an account takeover vulnerability in the customer password reset flow in system/controllers/forgot.php that allows unauthenticated attackers to brute-force the 6-digit otp_code. Attackers knowing a customer username can guess the code without attempt limits or lockout, then read the newly set password from the HTTP response to hijack the account.	9.1	More Details
CVE-2026-86706	The Quick quotes WordPress plugin through 1.0.0 does not perform any capability or nonce check on one of its AJAX actions and lets the caller choose which option is written, allowing unauthenticated users to alter arbitrary site settings and to make the site unavailable.	9.1	More Details
CVE-2026-81535	In wolfSSH through 1.5.0 built with --enable-fwd, DoChannelOpen() in src/internal.c gates only direct-tcpip channel opens with the forwarding policy callback. forwarded-tcpip opens are admitted without an authorization check and are not capped in number, allowing a malicious SSH peer to make an endpoint allocate unbounded per-channel buffers for forwarding channels the application never authorized. A client also does not check a forwarded-tcpip open against the forwards it registered with a tcpip-forward request, as RFC 4254 section 7.2 requires, so a malicious server can open forwarding channels for addresses and ports the client never asked it to forward.	9.1	More Details
CVE-2026-85121	The Insurify WordPress plugin through 1.0 does not have authorisation and nonce checks on one of its AJAX actions, allowing unauthenticated users to create and overwrite arbitrary WordPress options with request data, which can take the site offline and deactivate all of its Insurify WordPress plugin through 1.0.	9.1	More Details
CVE-2026-97720	Incorrect implementation of JWT/OAuth authentication in Impala executors in Apache Impala versions up to and including 4.5.2 which allows attacked to access resources served by the executor's webserver when that webserver is configured to accept JWT/OAuth tokens. Bearer token (JWT) signatures are not validated resulting in the webserver accepting any valid JWT. Users are recommended to either disable JWT/OAuth auth for Impala executors or upgrade to version 4.5.3, which fixes this issue.	9.1	More Details
CVE-2026-86717	The Insurify WordPress plugin through 1.0 does not have authorisation and nonce checks on one of its AJAX actions, allowing unauthenticated users to delete arbitrary WordPress options, which can take the site offline and strip every user of their role.	9.1	More Details
CVE-2025-70516	The websocket handler of Fanvil x7a firmware version 2.6.0.1182 does not enforce proper authentication restrictions against sessionless users. The lack of restrictions grants anyone the ability to view any device resources such as operational logs or perform diagnostic requests.	9.1	More Details
CVE-2026-62176	PraisonAI is a multi-agent teams system. Prior to version 4.6.78, the `deploy/api.py` module generates Python server code by directly interpolating the `agents_file` parameter into an f-string that is then written to a file and executed via `subprocess.Popen()`. An attacker who controls the `agents_file` value (via CLI argument, configuration, or upstream API) can inject arbitrary Python code. Version 4.6.78 patches the issue.	9.1	More Details
CVE-2026-108860	BotSharp through 5.2.0 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to forge bearer tokens using the hard-coded Jwt:Key in WebStarter appsettings.json. Attackers can sign tokens with the committed HMAC secret and fixed botsharp issuer and audience to impersonate any known user, including administrators, on Authorize-protected API routes.	9.1	More Details
CVE-2026-107510	An authenticated high privilege user can inject arguments in troubleshooting commands resulting in privilege escalation.	9.1	More Details
CVE-2026-81649	The Fundiin cho WooCommerce WordPress plugin through 3.4.0 does not have proper authorisation on several of its REST API routes, relying instead on a credential that is identical on every installation, allowing unauthenticated attackers to disclose the store's payment credentials and customer order data, overwrite the payment gateway configuration so that payments are credited elsewhere, and mark unpaid orders as paid. The same missing authorisation also allows arbitrary script to be stored in a field which is output unescaped on the classic checkout, leading to unauthenticated stored XSS on stores that do not use the block-based checkout.	9.1	More Details

CVE-2026-19218	Weak Password Recovery Mechanism for Forgotten Password vulnerability in AKIN Software Computer Import-Export Industry and Trade Co. Ltd. MyRezta allows Password Recovery Exploitation. This issue affects MyRezta: from 2.06.03 before 2.07.01.	9.1	More Details
CVE-2026-17609	The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Arbitrary Directory Deletion in all versions up to, and including, 6.3.316 via the submit_form function. This is due to insufficient validation of attacker-controlled JSON field declarations against the actual form schema, combined with a non-effective ABSPATH guard that dirname() trivially bypasses by stripping the trailing slash. This makes it possible for unauthenticated attackers to recursively delete arbitrary directories on the server, including the WordPress root directory. Exploitation requires that an administrator has enabled the 'Delete files from server after form submissions' setting, though this is a documented and commonly-enabled feature.	9.1	More Details
CVE-2026-107640	Integrics Enswitch 3.13 through 4.4 contains an authentication bypass vulnerability in /api/json/user/password/update/ that allows unauthenticated attackers to change account passwords by omitting the reset parameter. Attackers can target accounts with no pending reset, whose empty reset_key matches the defaulted empty value, to take over administrator accounts after enumerating valid usernames.	9.1	More Details
CVE-2026-88647	A hostname verification bypass in GnuTLS v3.8.13 allows attackers to circumvent the Common Name fallback mechanism and eavesdrop on communications via a crafted certificate.	9.1	More Details
CVE-2026-95210	Improper certificate validation in gnutls v3.8.13 causes the application to accept certificates containing invalid extensions.	9.1	More Details
CVE-2026-104076	TVU Networks Receiver/Transceiver devices running firmware before version 7.9 contain a missing authentication vulnerability that allows remote unauthenticated attackers to read sensitive device information and modify device configuration via unprotected REST API endpoints. Attackers can send unauthenticated GET requests to disclose network configuration, firmware details, and cloud service information, or issue POST requests to endpoints such as /Setting3/API/API/v1/LocalNetwork/DNS to alter DNS settings and enable man-in-the-middle attacks on outbound connections to TVU cloud infrastructure.	9.1	More Details
CVE-2026-16823	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote attacker to bypass security restrictions due to improper authentication.	9.1	More Details
CVE-2026-16916	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to execute arbitrary code due to a protection mechanism failure.	9.1	More Details
CVE-2026-19491	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote attacker to bypass authentication due to improper authentication.	9.1	More Details
CVE-2026-79842	An authentication bypass vulnerability exists in HPE Intelligent Management Center (iMC) prior to v7.3 E0713	9.1	More Details
CVE-2026-76483	As part of Cisco's ongoing commitment to proactive security and product quality, the engineering team for Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76483 are related to issues with insufficiently protected credentials that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-522.	9.1	More Details
CVE-2026-104801	The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the rename_files function in all versions up to, and including, 34.0.10 This makes it possible for unauthenticated attackers 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). The relocated file is moved byte-identically into the publicly accessible wp-content/uploads/ppom_files/confirmed/ directory, meaning the attack also results in arbitrary file read for any web-readable file on the server.	9.1	More Details
CVE-2026-	The Avada (Fusion) Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.16.1. This is due to the plugin not properly verifying authorization before dispatching a WordPress action hook whose name is taken from an attacker-supplied form-field value (via the notification email_message [field] placeholder and the {action_hook,...} dynamic-data token; the 3.16.1 trust gate is_content_request_supplied() only inspects \$_POST['args']/\$_GET['args'], never the \$_POST['formData'] the public form-submit endpoint parses). This makes it possible for unauthenticated attackers to invoke arbitrary WordPress action hooks (multiple per request), causing state changes up to permanent, irreversible destruction of site content: a verified unauthenticated request permanently deleted trashed posts, pages, and comments via the core wp_scheduled_delete action. Other non-deny-listed hooks extend	9.1	More Details

97670	the impact to denial of service (e.g. wp_maybe_auto_update) and, where vulnerable third-party handlers are installed, further privileged writes. The same unauthenticated dynamic-data pipeline additionally exposes a blind arbitrary user/post-meta read; the read result is delivered only to the site owner and is not attacker-exfiltrable through the plugin's own email/response paths. Exploitation requires a published Avada form with AJAX submission and a notification whose email_message template includes an [all_fields] or explicit [field] placeholder - the default form configuration.		
CVE-2026-78663	The HTTP/2 server can refund connection-level flow control twice for the same data: Once when a client resets a stream (refunding data for any sent-but-unread portion of the stream), and again when a request handler reads the buffered data. A malicious client can exploit this to bypass the configured connection-level flow control limit (MaxReceiveBufferPerConnection). Total buffered data is still limited by the concurrent stream limit and stream-level flow control.	9.1	More Details
CVE-2026-107645	The Blocksy Companion plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.1.58 This is due to the implement_user_registration() AJAX handler explicitly disabling Dokan's vendor-registration nonce check (via add_filter('dokan_register_nonce_check', '__return_false')) and then trusting an attacker-supplied \$_POST['role'] value when invoking wc_create_new_customer() and wc_set_customer_auth_cookie(). This makes it possible for unauthenticated attackers to elevate their privileges to a Dokan 'seller' (vendor) account — including sites where the Dokan vendor signup is explicitly turned off — and to be auto-authenticated into that account, which grants publishing capabilities beyond those of a normal customer.	9.1	More Details
CVE-2026-108264	Wizarr is an advanced user invitation and management system for Jellyfin, Plex, Emby, and other media servers. Prior to 2026.9.1, wizard step Markdown supplied through the editor or imported bundles was evaluated by app/blueprints/wizard/routes.py in the application's non-sandboxed Jinja2 environment with application globals exposed. An authenticated user able to create steps, or an administrator importing an untrusted bundle through POST /settings/wizard/import, could execute arbitrary Python when GET /wizard/{server}/{idx} rendered the stored step; app/jinja_filters.py and app/services/wizard_widgets.py contained additional evaluation sinks. This could execute operating-system commands as the application user, disclose the Flask SECRET_KEY, access connected service credentials and the database, and produce stored cross-site scripting. This issue is fixed in 2026.9.1.	9.1	More Details
CVE-2026-7826	A heap-based out-of-bounds read in the BufferSerializerIOv2_ReadBuffer function (src/serializers/serializer_io.c) in FalkorDB before 4.18.4 allows a remote attacker who can issue Redis replication commands (for example, against an instance with no password configured) to cause a denial of service or disclose heap memory by supplying a crafted RDB stream whose sub-buffer length field exceeds the remaining buffer size. The only bounds check is an ASSERT(), which is compiled out in release builds, so memcpy() reads past the end of the heap allocation.	9.1	More Details
CVE-2026-76454	A vulnerability in the Cisco Smart Licensing Utility API of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an unauthenticated, remote attacker to write arbitrary files to the system or cause a DoS condition on an affected application. This vulnerability is due to improper input validation and a lack of authentication in the management API. An attacker could exploit this vulnerability by sending a crafted request to the affected API. A successful exploit could allow the attacker to modify system files or cause a DoS condition.	9.1	More Details
CVE-2026-62025	Unauthenticated Arbitrary File Upload in Tailored Tools <= 3.0.3 versions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-106155	In Progress® Telerik® Report Server prior to version 12.2.26.1007, a stored cross-site scripting vulnerability in the shared reporting engine allows an authenticated report author to embed javascript: or vbscript: URLs in report navigation actions or HTML text box links. When another user views the malicious report and the embedded navigation is triggered, attacker-controlled script can execute in the web report viewer's origin. In a multi-user Report Server deployment, this can enable privilege escalation by performing actions in a higher-privilege user's authenticated session, including an administrator's session.	8.9	More Details
CVE-2026-104335	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper access control.	8.8	More Details
CVE-2026-62142	Cross-Site Request Forgery (CSRF) vulnerability in Melapress WP 2FA wp-2fa allows Cross Site Request Forgery.This issue affects WP 2FA: from n/a through 4.1.0.	8.8	More Details

CVE-2026-96227	The Piotnet Forms WordPress plugin through 1.0.30 does not authenticate or validate a form-submission file-upload request and permits browser-renderable file types to be stored, allowing unauthenticated attackers to store a file that executes arbitrary JavaScript in the site's origin when it is opened (Stored XSS).	8.8	More Details
CVE-2026-108113	ILIAS before 9.24, 10.12, and 11.5 contains an unrestricted file upload vulnerability in QTI question import image handling (ilQtiMatImageSecurity) that allows authenticated authors to write executable files. Attackers with question pool import rights can import a crafted archive writing a .htaccess and PHP file to the web-served image directory, achieving remote code execution as the web server user.	8.8	More Details
CVE-2026-87690	The Metasploit Framework post module post/apple_ios/gather/ios_image_gather is affected by a relative path traversal vulnerability (CWE-22). The module interpolates file names taken from a Meterpreter directory listing — data fully controlled by a hostile or tampered iOS device — directly into the local destination path passed to client.fs.file.download_file(), with no sanitization. The underlying stdapi sink (lib/rex/post/meterpreter/extensions/stdapi/fs/file.rb) writes to whatever path is supplied, so a listing entry such as ../../msfconsole.rc escapes the intended ~/.msf4/loot/<random> directory and overwrites ~/.msf4/msfconsole.rc, a resource file that every msfconsole invocation automatically executes at startup (lib/msf/ui/console/driver.rb:196). An attacker-controlled device that lures an operator into running this gather module achieves an arbitrary file write as the operator; because the written msfconsole.rc can load a second written file (a Ruby plugin whose top-level code runs on require), this converts into persistent code execution and an interactive shell as the operator (frequently root) on the pentester's workstation at the next console launch. The same traversal was previously fixed upstream in the recursive downloader (stdapi/fs/dir.rb scrubs separators); this module omitted the equivalent scrub. The fix applies the same separator scrub (or File.basename) to listing entries before building the local path.	8.8	More Details
CVE-2026-95534	Deserialization of Untrusted Data vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Object Injection. This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.19.	8.8	More Details
CVE-2026-15894	The Bluetooth Mesh On-Demand Private Proxy solicitation handler in subsys/bluetooth/mesh/solicitation.c copies a received Solicitation PDU into a fixed 17-byte stack buffer without bounding the source length. In sol_pdu_decrypt(), out is allocated as NET_BUF_SIMPLE(17) and then filled with net_buf_simple_add_mem(out, in->data, in->len); net_buf_simple_add() guards its tailroom only with __ASSERT_NO_MSG, which is compiled out in production builds, so when in->len > 17 the underlying memcpy writes attacker-controlled bytes past the 17-byte stack buffer. The copy occurs before any decryption or authentication, so no key material is required to trigger it. The oversized length arises because the mesh scan callback in subsys/bluetooth/mesh/adv.c calls net_buf_simple_restore() before dispatching to bt_mesh_sol_rcv(), leaving buf->len covering the entire remaining advertising payload rather than just the Solicitation Service Data. After the parser locates the Service Data AD and consumes the Identification Type byte, the remaining buf->len is the 17-octet Network PDU plus any trailing advertising bytes, and prior to this fix there was no maximum-length check (only a minimum). An attacker can therefore append extra AD structures or padding after the Solicitation Service Data to make buf->len exceed 17. bt_mesh_scan_cb() is registered directly as the BLE scan callback, so buf is raw, unauthenticated advertising data received over the air. Any device in radio range can send a non-connectable advertisement carrying a crafted mesh Proxy Solicitation to a node that has CONFIG_BT_MESH_OD_PRIV_PROXY_SRV enabled and is currently eligible to be solicited (GATT proxy disabled, On-Demand Private Proxy enabled), with no pairing, bonding, or provisioning. The result is an attacker-controlled stack overwrite — plausibly leading to remote code execution and at minimum a reliable remote denial of service. The fix trims buf->len to the spec-fixed 17 octets (dropping the PDU if fewer remain) before decryption.	8.8	More Details
CVE-2026-89091	A flaw was found in ansible-core. When installing a collection with `ansible-galaxy collection install`, the archive extractor validates member paths using lexical path normalisation (os.path.abspath) instead of resolving symbolic links (os.path.realpath), and it performs no containment check on symlink-typed directory members before creating them. A crafted collection tarball can chain symlink directory entries so that a subsequent file member is written outside the intended destination directory. This allows an attacker who can get a victim to install a malicious collection to overwrite arbitrary files with the privileges of the user running ansible-galaxy, leading to code execution on the control node. This is a bypass of the fix for CVE-2020-10691.	8.8	More Details
CVE-2026-107639	ILIAS before 9.24, 10.x before 10.12 and 11.x before 11.5 contains an argument injection vulnerability in asslimagemapQuestionGUI that allows question authors to inject ImageMagick convert options via uploaded image filenames. Attackers can embed tab-separated options, which escapeshellcmd() does not neutralise, to write a PHP file under the web root and achieve remote code execution.	8.8	More Details
CVE-2026-104766	The Appointment Booking Plugin - LatePoint Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 5.7.3. This is due to the `OsSettingsController::update()` handler iterating over attacker-supplied `settings` parameters without an allowlist of permitted setting names or values, and `OsSettingsHelper::prepare_value()` performing no role allowlist validation before persisting the `default_wp_role_for_customer` setting — a restriction that exists only in the UI dropdown and is never enforced server-side. This makes it possible for authenticated attackers holding a LatePoint role with the `settings__edit` capability (such as an agent or custom role) to overwrite the default WordPress role for new customers with `administrator`, causing any subsequently self-registered LatePoint customer account to be created with full WordPress administrator privileges. Exploitation requires	8.8	More Details

	that a WordPress administrator has granted the `settings__edit` capability to a LatePoint agent or custom role, and that a new customer account is registered through LatePoint after the malicious setting change is persisted.		
CVE-2026-107813	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, the api/cluster router exposes node and namespace mutation operations and cluster-wide Nginx reload or restart operations with AuthRequired but without RequireSecureSession. An authenticated OTP-enabled user possessing a stolen or persisted JWT can therefore perform node CRUD, read or replace node credentials, change namespaces, and invoke nodes/reload_nginx or nodes/restart_nginx without a fresh second-factor step-up. This issue is an incomplete fix for CVE-2026-84315 and is fixed in version 2.5.0.	8.8	More Details
CVE-2026-107811	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, ordinary authenticated users can access /api/nodes and /api/nodes/:id, whose responses serialize the node token field. The same token is accepted as X-Node-Secret by AuthRequired and maps the request to initUser, allowing the user to impersonate a trusted node against a reachable cluster member. This cross-node authentication bypass can expose sensitive management operations, including configuration synchronization and service restart. This issue is fixed in version 2.5.0.	8.8	More Details
CVE-2026-87683	Multiple stack-based buffer overflow vulnerabilities exist in the REST API management component of Brocade Fabric OS versions prior to 10.0.1. When processing API request payloads (such as device configuration attributes or port mapping requests) the REST API service fails to properly validate incoming array counts and string lengths against internal buffer capacities. An authenticated attacker with REST API access can transmit crafted, oversized request parameters to induce memory corruption on the execution stack. This may result in a denial-of-service condition (daemon crash) or potential arbitrary code execution within the management process context.	8.8	More Details
CVE-2026-17196	The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Unrestricted File Type Upload in all versions up to, and including, 6.3.316 via the upload_files function. This is due to missing file type validation in the upload_files function, which reads and applies an attacker-controlled extensions string from _super_elements post meta verbatim as the allowed MIME type map. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. The attack requires a preceding step: poisoning the _super_elements post meta via the super_save_form AJAX handler, which lacks a capability and nonce check but requires the attacker to be authenticated as at minimum a Subscriber-level user; the subsequent file upload via super_upload_files requires no authentication at all.	8.8	More Details
CVE-2026-87682	Multiple OS Command Injection vulnerabilities exist in the management interface and session processing routines of Brocade Fabric OS versions before 10.0.1. Input processing flaws during remote management connection validation and session verification for directory-based user accounts allow untrusted input containing shell metacharacters to reach internal system execution wrappers. An authenticated user or a compromised directory service account can exploit these vulnerabilities to execute arbitrary operating system commands with elevated privileges on the target device.	8.8	More Details
CVE-2026-96671	Cross-Site Request Forgery (CSRF) vulnerability in fifu.app Featured Image from URL featured-image-from-url allows Cross Site Request Forgery. This issue affects Featured Image from URL: from n/a through 6.0.7.	8.8	More Details
CVE-2026-87680	A command injection vulnerability in the REST API management interface of Brocade Fabric OS versions before 10.0.1 allows an authenticated user to execute arbitrary system commands via crafted input parameters.	8.8	More Details
CVE-2026-97188	The String locator WordPress plugin before 2.6.8 does not restrict the classes allowed when deserializing the content of a database row saved through its database editor, allowing unauthenticated attackers to store a serialized PHP object that is instantiated when an administrator later opens and saves that row. If a suitable POP chain is present via another installed String locator WordPress plugin before 2.6.8 or , this can lead to arbitrary file deletion, sensitive data disclosure or remote code execution.	8.8	More Details
CVE-2026-107809	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, AuthRequired accepts a browser-managed token cookie as an API credential after the front end stores the JWT in that cookie. Because management endpoints do not universally require a CSRF token or perform Origin or Referer validation, a remote attacker can induce a logged-in administrator's browser to submit authenticated cross-site state-changing requests, including POST /api/configs. The attack requires an administrator account without OTP/Passkey or a target endpoint that does not require secure-session proof. The attacker cannot read the cross-origin response but can modify Nginx configuration, trigger reloads, or invoke other management operations reachable with the victim's session. This issue is fixed in version 2.5.0.	8.8	More Details
CVE-2025-15700	The AWP Classifieds WordPress plugin before 4.4.9 does not validate the type of files extracted from an uploaded ZIP archive during its listing-import feature, allowing users with the AWP Classifieds WordPress plugin before 4.4.9's management capability to upload arbitrary PHP files to a publicly accessible, network-shared directory and achieve remote code execution.	8.8	More Details
CVE-	The Koinonia Link WordPress plugin before 1.1.5 does not check that a user is allowed to change roles before		More

2026-87782	saving a role selection submitted with a profile update, allowing any authenticated user, such as a subscriber, to grant themselves the Administrator role.	8.8	Details
CVE-2026-77183	The FooSales – Point of Sale (POS) for WooCommerce plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.43.0. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with FooSales Cashier-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	8.8	More Details
CVE-2025-70517	The request handler of Fanvil x7a firmware version 2.6.0.1182 does not enforce any cross-origin resource protection for any state-changing request performed against the applications. Due to the lack of protection, cross-origin boundary can be completely bypassed, allowing for Cross-Site Request Forgery Attacks against any endpoint.	8.8	More Details
CVE-2026-106059	GitAhead through 2.7.1 on macOS contains a command injection vulnerability that allows attackers to execute shell commands by crafting repository filenames interpolated unescaped into the Show in Finder AppleScript. Attackers can commit a file whose path contains a double quote followed by a do shell script payload, which runs as the victim user when Show in Finder is chosen.	8.8	More Details
CVE-2026-105885	Deserialization of Untrusted Data vulnerability in 10Web Slider by 10Web slider-wd allows Object Injection.This issue affects Slider by 10Web: from n/a through 1.2.62.	8.8	More Details
CVE-2026-108980	Blinko through 1.8.8 allows directory traversal, overwriting startup files as root, via installPlugin. It builds the plugin install path from an unsanitized name in server/routerTrpc/plugin.ts, and the plugin.installPlugin tRPC procedure is open to any authenticated user. Thus, a name containing ../ sequences writes the downloaded plugin files outside the plugins directory. Because the official Docker image runs as root, an authenticated attacker overwrites a root-owned startup file and achieves remote code execution as root. Self-registration for an account may be possible.	8.8	More Details
CVE-2026-107807	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, Nginx UI accepts the Node.Secret master credential through the node_secret query parameter in HTTP and WebSocket authentication paths instead of requiring the X-Node-Secret header. The credential can consequently appear in access logs, proxy logs, browser history, Referer headers, configuration URLs, and deployment environment data. A party that obtains the secret can bypass normal password, JWT, session, and second-factor checks and obtain persistent administrative API access, including access to configuration and secret material. This issue is fixed in version 2.5.0.	8.8	More Details
CVE-2026-103305	The Prenotazioni WordPress plugin through 1.7.5 does not have authorisation and CSRF checks when saving its settings, and does not escape some of them when outputting them, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against administrators and site visitors.	8.8	More Details
CVE-2026-19570	The LE Audio Broadcast Sink in subsys/bluetooth/audio/bap_broadcast_sink.c copies subgroup metadata from a received Basic Audio Announcement (BASE) into the static Broadcast Audio Scan Service parameter structure mod_src_param without any bounds check. In base_subgroup_meta_cb() the destination element was selected as mod_src_param.subgroups[mod_src_param.num_subgroups] with no test against ARRAY_SIZE(mod_src_param.subgroups) (sized by CONFIG_BT_BAP_BASS_MAX_SUBGROUPS, default 1), and the metadata was copied with memcpy() using the raw on-air length returned by bt_bap_base_get_subgroup_codec_meta() into a metadata array sized by CONFIG_BT_AUDIO_CODEC_CFG_MAX_METADATA_SIZE (default 4). The BASE validator bt_bap_base_get_base_from_ad() only checks structural consistency and permits up to ~24 subgroups and metadata LTVs of ~240 octets. The defect is reached from the periodic advertising receive callback: pa_recv() → bt_data_parse() → pa_decode_base() → update_recv_state_base() → bt_bap_base_foreach_subgroup() → base_subgroup_meta_cb(). Every broadcast sink registers a scan-delegator receive state at creation (bt_bap_broadcast_sink_create() calls broadcast_sink_add_src()), and CONFIG_BT_BAP_BROADCAST_SINK depends on CONFIG_BT_BAP_SCAN_DELEGATOR, so the path is active in every broadcast-sink build once the device is periodic-advertising-synced. An attacker in radio range who operates a broadcast source the device syncs to — or who impersonates the advertiser address and SID of one already in use, periodic advertising data being unauthenticated — can change the BASE at will; each new BASE is re-parsed. A crafted BASE therefore writes attacker-chosen bytes past the end of a fixed static object in .bss: up to roughly 236 bytes for an oversized metadata LTV, plus whole struct bt_bap_bass_subgroup records for each subgroup beyond CONFIG_BT_BAP_BASS_MAX_SUBGROUPS. This is memory corruption of adjacent Bluetooth-audio state reachable with no pairing, bonding or GATT connection, with a potential for remote code execution in the Bluetooth RX thread; in addition, the unvalidated metadata_len is forwarded to bt_bap_scan_delegator_mod_src(), which neither clamps it nor rejects it, leading to a further copy into the receive state and to out-of-bounds memory being disclosed in the BASS receive-state notification sent to a connected Broadcast Assistant. The fix rejects a BASE carrying more subgroups than the receive state can hold (discarding the update entirely) and omits metadata that does not fit rather than copying it, and additionally honours the previously-ignored error return of the subgroup decode pass.	8.8	More Details
	SkillHub before 0.2.22 contains an incorrect authorization vulnerability in AccountMergeService and		

CVE-2026-108550	AccountMergeController that allows authenticated attackers to take over other accounts by abusing the merge flow. Attackers can call the merge initiate endpoint with a target username or OAuth identity, receive the verification token directly, and confirm the merge to inherit the victim's API tokens, roles and namespace ownership.	8.8	More Details
CVE-2026-76453	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76453 are related to improper neutralization issues that are grouped under the Common Weakness Enumeration (CWE) CWE-707.	8.8	More Details
CVE-2026-106433	Improper state management in MongoDB libmongocrypt can cause provider-specific data to be treated as an incompatible type when cleaning up a key document containing duplicate masterKey fields. An authenticated actor who can modify key vault documents, or a server that returns such a key document, can cause invalid memory access and invalid frees in the client process. This can terminate the application or corrupt process memory.	8.8	More Details
CVE-2026-19569	dynamic_object_create() in kernel/userspace/userspace.c computed the backing allocation for a dynamically allocated kernel object as obj_size_get(otype) + size, and for thread stack elements as STACK_ELEMENT_DATA_SIZE(size) (a round-up plus fixed overhead), without checking either expression for unsigned wrap-around. A size close to SIZE_MAX makes the computed total wrap to a very small value, so the heap chunk handed out is a few bytes while the object descriptor is still tagged with the full requested type and registered in the kernel object table. The size argument reaches that arithmetic directly from user mode. k_object_alloc_size() is declared __syscall in include/zephyr/sys/kobject.h, its verifier z_vrfy_k_object_alloc_size() in kernel/userspace/userspace_handler.c is a bare pass-through, and z_object_alloc() only range-checks otype — nothing bounds size. The stack-element branch is additionally reachable through the k_thread_stack_alloc() syscall via kernel/dynamic.c. Because subsequent kernel-object validation checks only the object's type and initialization state, the undersized handle passes K_SYSCALL_OBJ_INIT()/K_SYSCALL_OBJ_NEVER_INIT(), and the matching init syscall (for example k_mutex_init(), k_sem_init(), or k_thread_create()) then writes a complete object over the truncated allocation. An unprivileged user-mode thread can therefore trigger a supervisor-mode out-of-bounds write into the kernel resource-pool heap, of a size and content it substantially controls, corrupting sys_heap chunk metadata and adjacent kernel objects. Under CONFIG_GEN_PRIV_STACKS the thread-stack branch additionally stores an attacker-influenced wild pointer as a user thread's privileged stack base. The practical result is escape from the CONFIG_USERSPACE sandbox — kernel-level code execution or at minimum kernel memory corruption and system compromise. Exploitation requires CONFIG_USERSPACE together with CONFIG_DYNAMIC_OBJECTS (also selected by CONFIG_DYNAMIC_THREAD under userspace), and a calling thread with an assigned resource pool. The fix rejects both overflowing computations and frees the partially built descriptor.	8.8	More Details
CVE-2026-108746	Vearch 3.5.2 through 3.5.9 contains an incorrect authorization vulnerability in Role.HasPermissionForResources that ignores stored ReadOnly or None privilege levels for resources listed in a role. Authenticated non-root users can upsert and delete documents with read-only access, or call PUT /roles to grant their role WriteRead privileges, escalating toward cluster administrator access.	8.8	More Details
CVE-2026-19083	Authorization bypass through User-Controlled key vulnerability in AKIN Software Computer Import-Export Industry and Trade Co. Ltd. OctoCloud allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects OctoCloud: from 1.12.06 before 1.12.07.	8.8	More Details
CVE-2026-76463	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76463 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-284.	8.8	More Details
CVE-2026-93548	The FooSales WordPress plugin before 1.43.3 does not verify that an authenticated caller is entitled to act as the user a request names, allowing any authenticated user to have the FooSales WordPress plugin before 1.43.3 act as an arbitrary other user, including an administrator, resulting in that user's account details being exposed and their account being taken over.	8.8	More Details
CVE-2026-108708	Wukong_HRM through commit 186115e contains a missing authorization vulnerability because EmployeeAspect assigns every caller the HR administrator role and EmployeeUtil data-scope checks return all employees. Any authenticated low-privileged employee can read payslips, salary records, bank cards and personal data, edit bank cards, and delete employees, departments and contracts company-wide.	8.8	More Details
CVE-2026-76470	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76470 are related to incorrect calculation issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-682.	8.8	More Details
CVE-	Satel Netco Design versions prior to v2.1.7 contains a relative path traversal vulnerability in its data export		

2026-101024	functionality. An authenticated user with Viewer privileges could write attacker influenced content to file system locations accessible to the application service. Successful exploitation could result in unauthorized file creation or modification and, under certain conditions, arbitrary code execution.	8.8	More Details
CVE-2026-105436	Deserialization of Untrusted Data vulnerability in MainWP MainWP Child mainwp-child allows Object Injection.This issue affects MainWP Child: from n/a through 6.2.1.	8.8	More Details
CVE-2026-103694	The Mobile builder WordPress plugin through 1.4.2 does not properly restrict which user meta keys a logged-in user can update through one of its REST routes, allowing any user with a self-registered account, such as a customer, to grant themselves the administrator role.	8.8	More Details
CVE-2026-76472	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-76472 are related to issues with improper neutralization of special elements that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-74.	8.8	More Details
CVE-2026-76484	As part of Cisco's ongoing commitment to proactive security and product quality, the engineering team for Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76484 are related to issues with insufficient protection against code injection that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-94.	8.8	More Details
CVE-2026-104723	The LifterLMS – WP LMS for eLearning, Online Courses, & Quizzes plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 10.2.1 via deserialization of untrusted input . This makes it possible for authenticated attackers, with custom-level access and above, 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. This vulnerability is only exploitable during lesson creation when a temporary lesson ID triggers the custom metadata path, and requires the attacker to hold a role with the edit_course capability, such as Instructor, Instructor's Assistant, LMS Manager, or Administrator.	8.8	More Details
CVE-2026-55797	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. From 2.11.0 until 3.3.15, 3.4.10, 3.5.4, and 3.6.0-rc2, the Argo CD repo-server is vulnerable to command injection when it clones, tests, or fetches an SSH Git repository configured with a proxy URL. The proxy host and port are embedded in an SSH ProxyCommand that is executed through a shell without neutralizing shell metacharacters. A user who can create or update a repository or repository credential template can supply a crafted proxy host to execute commands in the repo-server and access its Git, Helm, and OCI credentials. This issue is fixed in versions 3.3.15, 3.4.10, 3.5.4, and 3.6.0-rc2.	8.8	More Details
CVE-2026-103413	Improper input validation vulnerability in Apache Camel Karavan. When a deployment was started, Karavan unmarshalled a project's `kubernetes.yaml` and applied every resource it contained to the cluster without restricting the resource kinds, without rejecting security-sensitive pod options, and without pinning the target namespace. An authenticated user of any role could therefore have Karavan apply arbitrary Kubernetes resources within the reach of its service account, including pods requesting hostNetwork, hostPID, hostIPC, hostPath volumes, host ports, privileged containers, privilege escalation or added capabilities. This issue affects Apache Camel Karavan: from 4.0.0 before 4.22.1. Users are recommended to upgrade to version 4.22.1, which fixes the issue.	8.8	More Details
CVE-2026-108963	databasement before 1.8.2 allows remote code execution because it runs certain commands (e.g., mariadb-dump) with a database name that can be specified by any authenticated user. For example, --result-file=/app/public/index.php can write to index.php. In other words, quoting prevents OS command injection in mariadb-dump, but the argument injection alone is sufficient for code execution indirectly. NOTE: the project's composer.json file does not indicate an independently published databasement Composer package.	8.8	More Details
CVE-2026-104725	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.9 This is due to a missing ownership and capability check on the `user` parameter within the `process_edit()` function, which allows any authenticated user with the `edit_contacts` capability to reassign a contact record's linked WordPress user ID to any arbitrary account without requiring the `edit_users` or `promote_users` capabilities. This makes it possible for authenticated attackers, with sales_rep-level access and above, to escalate their privileges to administrator by linking a contact to an administrator's WordPress user ID, then creating a note containing the `{auto_login_link}` replacement tag to trigger generation of a valid auto-login permissions-key URL for the administrator-linked contact, and finally visiting that URL to authenticate as the targeted administrator. The auto-login URL is stored in the note content and is readable back by the attacker via the `view_notes` and `add_notes` capabilities that the sales_rep role holds by default.	8.8	More Details
CVE-	Deserialization of Untrusted Data vulnerability in ExpressTech Quiz And Survey Master quiz-master-next		More

CVE-2026-104392	allows Object Injection.This issue affects Quiz And Survey Master: from n/a through 11.2.7.	8.8	Details
CVE-2025-70522	The request handler of Fanvil x7a firmware version 2.6.0.1182 does not enforce any cross-origin resource protection for any state-changing request performed against the applications. Due to the lack of protection, cross-origin boundary can be completely bypassed, allowing for Cross-Site Request Forgery Attacks against any endpoint.	8.8	More Details
CVE-2026-103412	Improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Apache Camel Karavan. A project file name supplied through the project file API was used verbatim as a path segment when the project was written to the working copy for a Git commit, so a name containing `../` sequences caused the file content to be written outside the project directory, to any location writable by the Karavan process. An authenticated user of any role could use this to overwrite application configuration or files on the application classpath and so execute code in the Karavan container. This issue affects Apache Camel Karavan: from 3.18.0 before 4.22.1. Users are recommended to upgrade to version 4.22.1, which fixes the issue.	8.8	More Details
CVE-2026-76282	Improper Control of a Resource Through its Lifetime. Splunk addressed multiple internally identified vulnerabilities in Splunk Enterprise versions 10.4.3, 10.2.7, 10.0.10, and 9.4.15. The vulnerabilities are grouped by Common Weakness Enumeration (CWE), with one Common Vulnerabilities and Exposures (CVE) identifier assigned to each group. See Details for more information.	8.8	More Details
CVE-2026-109186	jshERP through 3.6 contains a mass assignment vulnerability in the UserController update handler that allows authenticated users to overwrite protected fields including tenant_id and password. Attackers can send a crafted PUT /user/update body to switch into another tenant on next login or overwrite other users' password hashes for account takeover.	8.8	More Details
CVE-2026-83540	When password or public key authentication is used with the Windows port of wolfSSHd, the Windows logon token acquired for one authenticated connection is not released before a token is acquired for a subsequent connection, resulting in user login poisoning between connections. A less privileged user with a valid account on the server can exploit this to force a login as a more privileged user. The vulnerability was introduced with the initial Windows port of wolfSSHd in wolfSSH version 1.4.15 and affects all versions through 1.5.0. Non-Windows builds of wolfSSHd are not affected.	8.8	More Details
CVE-2026-104084	SmarterMail before build 9777 contains a privilege escalation vulnerability where JWT access and refresh tokens embed a role claim at issuance that is not revalidated against the account's current role when redeemed through POST /api/v1/auth/refresh-token. Attackers who capture a refresh token issued before an administrator demotion, or a demoted user whose session was not actively polling at the time of demotion, can replay the stale token to obtain a new access token retaining the higher-privilege role (such as DomainAdmin or SysAdmin) until natural token expiry.	8.8	More Details
CVE-2026-107375	JHipster is a development platform to quickly generate, develop, and deploy modern web applications and microservice architectures. From 7.0.0 until 9.4.0, reactive applications generated with Spring WebFlux, Spring Data R2DBC, and a SQL database pass the attacker-controlled sort request parameter from paginated entity-list endpoints into createOrderByFields in generators/spring-boot/generators/data-relational/templates/src/main/java/package/repository/EntityManager_reactive.java.ejs. The generated code renders these properties into the SQL ORDER BY clause without validation or quoting, and the R2DBC simple query protocol can execute additional statements separated by semicolons. A normal authenticated user can consequently read sensitive tables, modify or delete data, or drop tables, while non-reactive JPA applications and NoSQL backends are outside this root cause. This issue is fixed in 9.4.0.	8.8	More Details
CVE-2026-86798	The HootBoard WordPress plugin through 3.1.4 does not perform any authorisation check on some of its REST endpoints, and does not escape the values stored through them before outputting them in a public page, allowing unauthenticated users to inject arbitrary web scripts that will execute in the browser of anyone visiting that page, including administrators.	8.8	More Details
CVE-2026-87760	The Web Vitals Tracking WordPress plugin through 5.4.2 does not validate or escape performance measurements submitted by unauthenticated visitors before storing them and outputting them in a script context on an administrative page, allowing unauthenticated attackers to perform Stored Cross-Site Scripting attacks against administrators.	8.8	More Details
CVE-2026-93675	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote attacker to execute arbitrary code due to an expected dependency confusion.	8.8	More Details
CVE-2026-88905	The KeyWord Collector WordPress plugin through 1.4 does not have any authorisation or nonce check when saving its settings, and does not escape them before output, allowing unauthenticated attackers to store malicious JavaScript that executes when an administrator opens the KeyWord Collector WordPress plugin through 1.4's settings page or when a visitor loads a page displaying its output.	8.8	More Details
CVE-2026-109185	jshERP through 3.6 contains a missing authorization vulnerability in the UserController updateUser handler that allows authenticated users to assign arbitrary roles to any user. Low-privilege attackers can send their own user id with the tenant administrator roleid to escalate privileges or rebind other tenant users' roles.	8.8	More Details

CVE-2026-88903	The Topcontent WordPress plugin through 1.2.1 does not properly authorise one of its request handlers and disables HTML sanitisation before storing the submitted content, allowing unauthenticated attackers to publish arbitrary posts containing malicious JavaScript on any site where its API key has never been configured.	8.8	More Details
CVE-2026-87764	The BuddyPress Instant Chat WordPress plugin through 1.6 does not check that the sender of a chat message belongs to the conversation it is being added to, nor does it escape message content before outputting it back, allowing unauthenticated users to store arbitrary web scripts that will execute in the session of any member who later views that conversation.	8.8	More Details
CVE-2026-97679	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command ('Code Injection') related to improper input validation.	8.8	More Details
CVE-2026-97678	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper input validation.	8.8	More Details
CVE-2026-87762	The Advised Web Push Notification WordPress plugin through 2.5.7 does not have authorisation checks on several state-changing operations, and the secret comparison it uses instead can be bypassed on installations where the secret key has never been set, allowing unauthenticated users to store arbitrary JavaScript that is executed in the browser of every site visitor.	8.8	More Details
CVE-2026-97676	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in code, resulting in a sandbox escape.	8.8	More Details
CVE-2026-88827	The Disable Users WordPress plugin through 1.0.5 does not enforce its account-disabling control on all authentication paths, allowing the holder of an account an administrator has disabled to continue authenticating with the account's full privileges.	8.8	More Details
CVE-2026-97673	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper input validation.	8.8	More Details
CVE-2026-88826	The SmugMug Embed WordPress plugin through 3.13 does not have authorisation or CSRF checks on an AJAX action that stores gallery data, and does not sanitise or escape that data before outputting it, allowing unauthenticated users to store arbitrary web scripts that execute when an administrator views the SmugMug Embed WordPress plugin through 3.13's settings screen.	8.8	More Details
CVE-2026-97655	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote attacker to execute arbitrary code due to an incomplete blocklist in the code security scanner.	8.8	More Details
CVE-2026-83742	Unsigned integer underflow in wstrncat() in src/port.c in wolfSSL wolfSSH from v1.4.11 through v1.5.0 on non-Windows platforms allows an authenticated remote attacker to write one out-of-bounds null byte past the end of a stack buffer by sending a crafted SFTP path. wolfSSH_RealPath() in src/ssh.c appends each path component with a remaining-size bound (outSz - curSz) rather than the full destination size, so once the accumulated path reaches half the output buffer the size_t computation n - strlen(s1) - 1 wraps to near SIZE_MAX. The strncat() call is then effectively unbounded and copies the whole component; when that component exactly fills the remainder of the buffer, its terminating null is written one byte past the end. The caller's own length check keeps the copied data inside the buffer, so the overflow is limited to that single null byte, which may corrupt an adjacent stack value and crash the process. Applications that call the public wolfSSH_RealPath() with an output buffer smaller than the input path are additionally exposed to an unbounded copy, because the word32 expression outSz - segSz in that length check also wraps.	8.8	More Details
CVE-2026-84261	The click5 CRM add-on to Contact Form 7 WordPress plugin through 1.0.4 does not sanitise and escape content submitted through an unauthenticated endpoint before outputting it back in an admin page, leading to Stored XSS which could be used against high privilege users such as admin.	8.8	More Details
CVE-2026-84260	The click5 CRM add-on to Gravity Forms WordPress plugin through 1.0.3 does not sanitise and escape content submitted through an unauthenticated endpoint before outputting it back in an admin page, leading to Stored XSS which could be used against high privilege users such as admin.	8.8	More Details
CVE-2026-94065	Deserialization of Untrusted Data vulnerability in BuddhaThemes ColorFolio colorit allows Object Injection.This issue affects ColorFolio: from n/a through 1.3.	8.8	More Details
CVE-2026-104629	A component loading mechanism in openPDC and openHistorian will construct and run any specified type, which may be an invalid component to load. An attacker with an authenticated user account and the ability to place a file on the host filesystem can use this to run arbitrary constructor code, and this code runs with	8.8	More Details

	the privileges of the affected service account.		
CVE-2026-84258	The click5 CRM add-on to Ninja Forms WordPress plugin through 1.0.1 does not sanitise and escape content submitted through an unauthenticated endpoint before outputting it back in an admin page, leading to Stored XSS which could be used against high privilege users such as admin.	8.8	More Details
CVE-2026-94064	Deserialization of Untrusted Data vulnerability in BuddhaThemes Neo Barber Shop WordPress Theme neocut allows Object Injection.This issue affects Neo Barber Shop WordPress Theme: from n/a through 3.5.	8.8	More Details
CVE-2026-84259	The click5 CRM add-on to WPForms WordPress plugin through 1.0.3 does not sanitise and escape content submitted through an unauthenticated endpoint before outputting it back in an admin page, leading to Stored XSS which could be used against high privilege users such as admin.	8.8	More Details
CVE-2026-18740	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to perform unauthorized actions due to argument injection.	8.8	More Details
CVE-2026-83526	The FV Player 8 plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 8.1.7 via the check_mimetype function. This is due to insufficient file type validation in check_mimetype(), which writes attacker-supplied remote file content to the public uploads directory before any MIME or extension check, combined with a missing capability check on new player creation. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. This requires successfully exploiting a race condition.	8.8	More Details
CVE-2026-103903	An incorrect authorization vulnerability in the WinBox authentication flow of MikroTik RouterOS allows a remote authenticated attacker with credentials for a low-privilege account permitted to use WinBox to obtain the authorization policy of a different existing account. The stage-one EC-SRP challenge and proof are verified using the attacker's account, while the independently supplied stage-two username is used to install the target account's privileges. By specifying a higher-privilege account such as admin, a low-privilege user can obtain a full administrative session without knowing the target account's password and can use that session to increase the privileges of the attacker's own account.	8.8	More Details
CVE-2026-105407	An OS Command Injection vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to execute arbitrary commands on the server.	8.8	More Details
CVE-2026-52903	A deserialization of untrusted data vulnerability was found in ManageIQ. The YamlLoadAliases module overrides YAML.safe_load to silently fall back to YAML.unsafe_load in production when a Psych::DisallowedClass error occurs. An authenticated attacker with dialog import access can exploit this to achieve remote code execution by uploading a crafted YAML payload that triggers the fallback and deserializes arbitrary Ruby objects. Red Hat CloudForms, which was based on ManageIQ, has reached End of Life and is no longer supported. No errata or patches will be issued. This CVE is being assigned for the benefit of the ManageIQ community and downstream consumers.	8.8	More Details
CVE-2026-87780	The LTL Freight Quotes WordPress plugin before 4.2.19 does not sanitise and escape values submitted through an unauthenticated endpoint before storing them and outputting them back in an administrative page, leading to Stored XSS which will execute in the session of any administrator viewing it.	8.8	More Details
CVE-2026-106558	Backstage is an open framework for building developer portals. Prior to 1.14.8, 1.15.6, and 2.0.1, the @backstage/plugin-techdocs-node package improperly validated mapping-style markdown_extensions configuration. An authenticated attacker who can register or influence an SCM-backed documentation source may bypass TechDocs sanitization and cause Python objects to be imported and instantiated in the generator runtime, leading to arbitrary code execution. Earlier fixes in versions 1.14.6 and 1.15.4 did not fully address the supported mapping representation of markdown_extensions. Impact is greatest when documentation generation runs with backend credentials, filesystem access, or internal network access. This issue is fixed in versions 1.14.8, 1.15.6, and 2.0.1.	8.8	More Details
CVE-2026-88962	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of code generation.	8.8	More Details
CVE-2026-19482	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of command arguments.	8.8	More Details
CVE-2026-62021	Subscriber PHP Object Injection in Angio <= 1.1.1 versions.	8.8	More Details
CVE-2026-105408	A Stored Cross-site Scripting (XSS) vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to execute arbitrary script code in user's browser session.	8.7	More Details

CVE-2026-105410	A Stored Cross-site Scripting (XSS) vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-78355	A path traversal vulnerability in the OTRS SendSupportBundle functionality allows an authenticated administrator to reference file paths outside the intended directory. This may allow files accessible to the OTRS application process to be deleted. The vulnerability does not bypass operating system file permissions. On OTRS versions prior to OTRS 7, the effective permissions of the web server process are relevant. Starting with OTRS 7, access is limited by the permissions of the dedicated OTRS user. Files with overly permissive ownership or file system permissions may therefore also be affected. The affected functionality may additionally attempt to include controlled files in a support bundle. However, support bundles are sent to a predefined OTRS support address, and direct disclosure of arbitrary files to the attacker has not been demonstrated. An attacker therefore requires valid administrative access to exploit the vulnerable functionality. The primary demonstrated impact is the deletion of files outside the intended directory within the effective permissions of the OTRS application process. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	8.7	More Details
CVE-2026-83943	Exposure of sensitive information to an unauthorized actor in Azure API Center allows an unauthorized attacker to disclose information over a network.	8.7	More Details
CVE-2026-105409	A Stored Cross-site Scripting (XSS) vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-88930	The Social Web Suite WordPress plugin through 4.1.12 does not require its shared secret to be set before accepting requests authorised by it, and does not sanitise and escape a parameter before using it in an SQL statement, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-103695	The Mobile builder WordPress plugin through 1.4.2 does not sanitise and escape a parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-89287	The ASPL Product Quotation WordPress plugin through 1.1.0 does not sanitize and escape a parameter before using it in SQL statements, allowing unauthenticated attackers to perform SQL injection and read arbitrary data from the database.	8.6	More Details
CVE-2026-89195	The Site Setup Wizard WordPress plugin through 1.5.8 does not properly sanitise and escape a parameter before using it in a SQL statement, which allows unauthenticated attackers to perform SQL injection attacks and read data from the database.	8.6	More Details
CVE-2026-89213	The Llavero.io WordPress plugin through 0.1.4 does not properly sanitise and escape a parameter before using it in a SQL statement, which allows unauthenticated attackers to perform SQL injection attacks and read data from the database.	8.6	More Details
CVE-2026-89214	The WpCues Basic Quiz WordPress plugin through 1.6.5 does not properly sanitise and escape values before using them in a SQL statement, which allows unauthenticated attackers to perform SQL injection attacks and read data from the database.	8.6	More Details
CVE-2026-89232	The Recordbrowser WordPress plugin through 1.1.7 does not sanitise and escape a parameter before using it in a SQL query, allowing unauthenticated attackers to append additional SQL queries and extract sensitive information from the database.	8.6	More Details
CVE-2026-87781	The LTL Freight Quotes WordPress plugin before 4.2.19 does not sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users.	8.6	More Details
CVE-2026-89234	The WP-Partner WordPress plugin through 1.2.1 does not sanitise and escape a parameter before using it in a SQL query, allowing unauthenticated attackers to append additional SQL queries and extract sensitive information from the database.	8.6	More Details
CVE-2026-107205	LMCache through 0.5.5 contains a missing authentication vulnerability in the multiprocess coordinator that allows remote unauthenticated attackers to access its HTTP fleet control API listening on all interfaces by default. Attackers can register or deregister instances via /instances, overwrite quotas via /quota endpoints, inject events via /events, and enumerate /directory/keys to disrupt caching and disclose placement metadata.	8.6	More Details
CVE-2026-89302	The Post Voting System WordPress plugin through 1.0 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details

CVE-2026-89299	The WP Verify API WordPress plugin through 1.0.0 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-89283	The WP Posts Password Batch Manager WordPress plugin through 1.1 does not perform any capability or nonce check on a bulk post-password action that runs on an always-loaded admin handler, allowing unauthenticated attackers to reset or overwrite the password of every published post, disclosing password-protected content or locking all posts behind an attacker-chosen password.	8.6	More Details
CVE-2026-89285	The Datalist it WordPress plugin through 0.0.3 does not sanitize and escape several request parameters before using them to build a SQL query, allowing unauthenticated attackers to perform SQL injection and read arbitrary data from the database.	8.6	More Details
CVE-2026-89297	The Loja Automática WordPress plugin through 1.0.0 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-81420	The Tcard WP WordPress plugin through 1.8.0 does not sanitise and escape a parameter before using it in a SQL statement in one of its unauthenticated AJAX actions, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-76458	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76458 are related to improper handling of exceptional conditions issues that are grouped under the Common Weakness Enumeration (CWE) CWE-703.	8.6	More Details
CVE-2026-81932	IBM Guardium Data Protection 12.0, 12.1, and 12.2 is vulnerable to SQL injection. A remote unauthenticated attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	8.6	More Details
CVE-2026-76456	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76456 are related to improper input validation of special elements used in a command issue that are grouped under the Common Weakness Enumeration (CWE) CWE-20.	8.6	More Details
CVE-2026-76457	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco NX-OS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76457 are related to out-of-bounds read issues that are grouped under the Common Weakness Enumeration (CWE) CWE-125.	8.6	More Details
CVE-2026-16163	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause memory corruption due to an out-of-bounds write.	8.6	More Details
CVE-2026-16159	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to obtain sensitive information and cause a denial of service due to an out-of-bounds write.	8.6	More Details
CVE-2026-93449	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of code generation.	8.5	More Details
CVE-2026-96329	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in tagDiv tagDiv Opt-In Builder td-subscription allows Blind SQL Injection.This issue affects tagDiv Opt-In Builder: from n/a through 1.7.6.	8.5	More Details
CVE-2026-62117	Subscriber SQL Injection in Barcode Scanner with Inventory & Order Manager <= 1.13.1 versions.	8.5	More Details
CVE-2026-107815	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the CONNECT engine's DOS table type used an incorrect boundary check that permitted a one-byte null write beyond a stack buffer at an attacker-controlled offset. An authenticated user able to use the CONNECT engine could cause a crash and potentially remote code execution. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	8.5	More Details
CVE-2026-95599	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Taskbuilder Taskbuilder taskbuilder allows Blind SQL Injection.This issue affects Taskbuilder: from n/a through 6.0.5.	8.5	More Details

CVE-2026-42633	Subscriber SQL Injection in Events Manager <= 7.4.6 versions.	8.5	More Details
CVE-2026-95610	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UpSolution UpSolution Core us-core allows Blind SQL Injection.This issue affects UpSolution Core: from n/a through 9.3.	8.5	More Details
CVE-2026-95607	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VibeThemes WPLMS wplms allows Blind SQL Injection.This issue affects WPLMS : from n/a through 4.973.	8.5	More Details
CVE-2026-42712	Subscriber SQL Injection in Qode Tours <= 3.1.3.2 versions.	8.5	More Details
CVE-2026-94663	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Blind SQL Injection.This issue affects ProfileGrid: from n/a through 6.0.0.2.	8.5	More Details
CVE-2026-107818	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the mariadb.service unit used /run/mysqld/wsrep-new-cluster during the next service restart. A database user with FILE privilege and a secure-file-priv configuration permitting writes to /run/mysqld could create that file and inject attacker-controlled environment values into the restarted service. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	8.4	More Details
CVE-2026-84250	IBM Guardium Data Protection 12.2 is vulnerable due to weak cryptographic protection and a hard-coded recovery key in the pkcrypto passkey component. A local attacker could exploit this vulnerability to recover the root password and gain root privileges.	8.4	More Details
CVE-2026-107814	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, MariaDB RPM packages created the dedicated mysql service account with the database data directory as its home directory. A database user with the FILE privilege could write startup dot-files such as .bash_profile into \$HOME, and those files could execute when an administrator opened a login shell for the mysql account. Debian packages are not affected because they use /nonexistent as the account home. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	8.4	More Details
CVE-2026-39453	Navigating to a certain URL on the switch's web server causes the switch to reboot. This can be automated using a tool like curl to create DoS conditions where the switch constantly reboots.	8.3	More Details
CVE-2026-108522	A vulnerability was found in Studio-Saelix Sencho up to 0.94.1. This affects an unknown part of the file /api/auth/login of the component Login Endpoint. Performing a manipulation of the argument X-Forwarded-For results in improper authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The patch is named 79b86ddcd4aefdd6941f098e35990ab397b13c72. To fix this issue, it is recommended to deploy a patch. The vendor confirms: "The login limiter relied on client-supplied X-Forwarded-For data without an explicit trusted-proxy boundary, allowing an attacker to rotate the apparent client address. The remediation now ignores forwarding headers by default, accepts them only from explicitly configured proxy CIDRs, and adds a separate failed-attempt limit keyed by normalized account identity."	8.3	More Details
CVE-2026-97680	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information or inject malicious data due to improper access control in the vertex result caching subsystem.	8.3	More Details
CVE-2026-108740	GoatCounter through 2.7.0 contains a mass assignment privilege escalation vulnerability in the userPrefSave handler that allows logged-in users to modify protected account fields via form-encoded requests. Attackers with read-only access can POST user.access[all]=* and user.email_verified=true to /user/pref, bypassing readonly tags to gain superuser or admin access.	8.3	More Details
CVE-2026-107376	webonyx graphql-php is a PHP implementation of the GraphQL specification. Prior to 15.32.3, GraphQL\Language\Parser performs recursive descent without a recursion limit in parseSelectionSet, parseValueLiteral, and parseTypeReference. A remote attacker can submit deeply nested selection sets, object or list values, or list types that exhaust the PHP process stack during pre-validation parsing, before query validation and complexity controls run. The resulting SIGSEGV can terminate PHP-FPM workers or long-running Swoole, RoadRunner, ReactPHP, or CLI processes and cannot be caught by application-level exception handling. This issue is fixed in version 15.32.3.	8.2	More Details
CVE-2026-82211	The Nexi XPay Build WordPress plugin through 7.6.2 does not verify the payment result supplied to several of its unauthenticated routes, allowing attackers to mark arbitrary orders as paid or failed, to cancel them, and to obtain order keys which expose guest buyers' details.	8.2	More Details

CVE-2026-17189	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session	8.2	More Details
CVE-2026-90983	Use of Client-Side authentication vulnerability in Hayat Health Facilities Inc. (Hayat Hospital) Hayat Mobile allows Authentication Bypass. This issue affects Hayat Mobile: from 3.3.0 before 3.4.0.	8.2	More Details
CVE-2026-96341	Incorrect Privilege Assignment vulnerability in WPMU DEV Forminator forminator allows Privilege Escalation.This issue affects Forminator: from n/a through 1.57.3.	8.2	More Details
CVE-2026-14496	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to a heap-based buffer overflow.	8.2	More Details
CVE-2026-15824	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to a heap-based buffer overflow.	8.2	More Details
CVE-2026-107701	dot-access through 1.0.0 contains a prototype pollution vulnerability that allows attackers to modify Object.prototype by supplying a crafted dotted path to set(). Attackers controlling the path, such as through user-supplied field names, can use __proto__ segments to inject properties into all objects, altering authorization flags and option defaults or crashing the process.	8.2	More Details
CVE-2026-76468	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76468 are related to improper input validation that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-20.	8.2	More Details
CVE-2026-14905	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	8.2	More Details
CVE-2026-107837	RIOT is an open-source microcontroller operating system designed for Internet of Things devices and other embedded systems. In 2026.07 and earlier, _receive() in sys/net/gnrc/network_layer/sixlowpan/gnrc_sixlowpan.c can route an undersized packet into SFF fragment handling after only a minimal payload check. The code then interprets the packet as a sixlowpan_frag_t or larger fragment header without verifying that the packet snip contains the required bytes. A remote attacker can send a malformed 6LoWPAN fragment that causes gnrc_sixlowpan_frag_rcv() to read beyond the packet buffer, potentially disclosing memory and crashing the network stack. No fixed repository release is available as of this review.	8.2	More Details
CVE-2026-108758	Easy!Appointments through 1.6.0 contains an authorization bypass vulnerability in Booking::register() that allows unauthenticated attackers to modify any appointment by supplying an appointment id without its hash. Attackers can enumerate sequential appointment ids with a self-asserted manage_mode flag to rewrite appointment details, rebind them to attacker-controlled customers, and obtain management hashes for rescheduling or cancellation.	8.2	More Details
CVE-2026-108865	AmoyLab Unla through 0.10.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to obtain valid access tokens because the OAuth2 server never authenticates a resource owner. Attackers can register a client, request a code from /authorize, and exchange it at /token to access OAuth2-protected MCP prefixes, proxied upstream APIs and injected credentials.	8.2	More Details
CVE-2026-108259	Tina is a headless content management system. Prior to 3.0.0, @tinacms/cli reads Git branch values from VERCEL_GIT_COMMIT_REF, GITHUB_BRANCH, or HEAD, incorporates the raw value into the API URL, and interpolates that URL into JavaScript string literals in packages/@tinacms/cli/src/next/codegen/index.ts and packages/@tinacms/cli/src/next/codegen/codegen/plugin.ts. A crafted Git-valid branch name containing a quote can terminate the generated string and inject an expression that executes when the generated client module is imported during a preview build. The injected code runs with the build process privileges and can read environment credentials, modify deployment artifacts, or make network requests. This issue is fixed in version 3.0.0.	8.2	More Details
CVE-2026-77214	libexpat before commit 13c5f63 contains a heap buffer over-read vulnerability in xmlparse.c. XML_ParseBuffer advances the parse buffer end with parser->m_bufferEnd += len using a caller-supplied length that is not validated against the allocated buffer size, so repeated XML_ParseBuffer calls move m_bufferEnd past the end of the heap allocation and subsequent parsing reads out of bounds. Reaching this path requires a parse buffer to already be present; otherwise XML_ParseBuffer returns XML_ERROR_NO_BUFFER. A buffer is present after a prior call to XML_GetBuffer, either directly (the common case) or indirectly through a prior XML_Parse call that allocates the buffer internally. The over-read discloses	8.2	More Details

	adjacent heap memory to the calling application, recovering heap pointers, libc function pointers, and code pointers sufficient to defeat ASLR and build further exploitation primitives.		
CVE-2026-62066	Unauthenticated Local File Inclusion in Volos <= 1.2 versions.	8.1	More Details
CVE-2026-62065	Unauthenticated Local File Inclusion in Cardea <= 2.3 versions.	8.1	More Details
CVE-2026-108628	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the saveDeptRolePermission endpoint of SysDepartPermissionController that allows any authenticated user to modify department role permissions. Low-privileged attackers can submit roled and permissionIds values to grant arbitrary menu or button permissions, escalating privileges or revoking other users' permissions.	8.1	More Details
CVE-2026-62096	Unauthenticated Local File Inclusion in Biolife <= 3.2.3 versions.	8.1	More Details
CVE-2026-62094	Unauthenticated Local File Inclusion in TechOne <= 3.0.3 versions.	8.1	More Details
CVE-2026-62067	Unauthenticated Local File Inclusion in Kaven <= 1.2 versions.	8.1	More Details
CVE-2026-94538	The WP File Download plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.3.9. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to permanently delete any file managed by WP File Download, empty the entire trash, move files between categories, and publish or unpublish arbitrary files.	8.1	More Details
CVE-2026-62092	Unauthenticated Local File Inclusion in Armania <= 1.4.8 versions.	8.1	More Details
CVE-2026-62068	Unauthenticated Local File Inclusion in Teoro <= 1.1 versions.	8.1	More Details
CVE-2026-62069	Unauthenticated Local File Inclusion in Fabius <= 1.0 versions.	8.1	More Details
CVE-2026-62075	Unauthenticated Local File Inclusion in Backhoe <= 2.0 versions.	8.1	More Details
CVE-2026-62070	Unauthenticated Local File Inclusion in Flipmart <= 2.8 versions.	8.1	More Details
CVE-2026-94257	The SMS Alert WordPress plugin before 4.0.1 does not bind the account whose password is being changed to the phone number that was actually verified during its OTP password reset, allowing unauthenticated attackers to set a new password on an arbitrary account, including an administrator, by verifying a one-time code sent to a phone number they control.	8.1	More Details
CVE-2026-42704	Unauthenticated Local File Inclusion in Kids Care <= 3.2.4 versions.	8.1	More Details
CVE-2026-62099	Unauthenticated Local File Inclusion in Boutique <= 2.3.3 versions.	8.1	More Details
CVE-2026-62115	Unauthenticated Local File Inclusion in KuteShop <= 4.2.9 versions.	8.1	More Details
CVE-	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysTenantController passApply handler that allows any authenticated user to approve tenant administrator applications. Attackers can file a		More

2026-108657	pending application via doApplyTenantPackUser and approve it through PUT /sys/tenant/passApply to gain tenant administrator pack permissions in any tenant.	8.1	Details
CVE-2026-108549	cc-connect through 1.5.0 contains a missing authentication vulnerability in the MAX platform adapter webhook mode in platform/max/max.go that accepts unauthenticated updates when no webhook_secret is configured. Remote attackers reaching the webhook listener on port 8080 can forge updates with an allowed or admin user_id to run privileged commands like /shell on the host.	8.1	More Details
CVE-2026-107384	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. From 3.2.0 until 3.2.5, 3.3.4, 3.4.7, and 3.5.4, applications that enable permitSetMultiParamEntries can pass objects whose keys are expanded into a SQL SET clause without being processed by escapeld. An attacker-controlled key containing a backtick can close the quoted identifier and cause the remainder of the key to be interpreted as SQL. This can update columns the application did not intend to expose and can append arbitrary SQL with the database user's privileges. The option is disabled by default, and serialized-object handling used when it is disabled is not affected. This issue is fixed in versions 3.2.5, 3.3.4, 3.4.7, and 3.5.4.	8.1	More Details
CVE-2026-94256	The SMS Alert WordPress plugin before 4.0.1 does not verify that the account being logged in is the one the verified one-time code belongs to, allowing unauthenticated attackers to sign in as any user with a stored phone number, including an administrator, by completing a code challenge on a phone they control.	8.1	More Details
CVE-2026-40777	Subscriber Broken Access Control in WPSection <= 1.5.1 versions.	8.1	More Details
CVE-2026-40801	Subscriber Broken Access Control in Wordable <= 8.2.10 versions.	8.1	More Details
CVE-2026-66566	Unauthenticated Local File Inclusion in Ambient <= 1.7 versions.	8.1	More Details
CVE-2026-104759	The WPO365 SEAMLESS WORDPRESS + MICROSOFT INTEGRATION (WPO365 LOGIN) plugin for WordPress is vulnerable to Authentication Bypass via OIDC Nonce Replay in all versions up to, and including, 44.1 This is due to `Id_Token_Service_Deprecated::process_openidconnect_token()` using the incompatible WordPress core `wp_verify_nonce()` function to validate a nonce produced by `Nonce_Service::create_nonce()` — a 64-character hex value that `wp_verify_nonce()` can never successfully verify — causing the nonce check to silently fail without terminating authentication, so execution continues into `authenticate_oidc_user()` with the attacker-supplied `id_token`. This makes it possible for unauthenticated attackers who have obtained a previously-issued, valid `id_token` for a target account to replay that token and authenticate as any WordPress user, including administrators, resulting in full site takeover. This vulnerability is only exploitable when the `use_id_token_parser_v2` plugin option is enabled, as this is the configuration that routes token processing through the deprecated parser containing the broken nonce check.	8.1	More Details
CVE-2026-107333	Malcolm's nginx based reverse proxy contains a URL path normalization inconsistency between its Lua based role-based access control (RBAC) authorization layer and nginx's own request routing logic. An authenticated user can craft a specially formatted request path to bypass role-based restrictions and reach administrative or role gated endpoints they should not have access to. This affects all restricted paths protected by the RBAC authorization layer, including file upload, PHP server, htadmin, and authentication management interfaces.	8.1	More Details
CVE-2026-62251	Homer is open source telecom observability software. Prior to version 11.0.283, the `V4StatisticsQuery` handler passes the user-supplied `rawquery` field directly to DuckDB without calling the `sqlvalidator.ValidateRawSQL` function used throughout the rest of the codebase. Any authenticated user can execute arbitrary SQL statements against all data accessible through the FlightSQL service. Version 11.0.283 patches the issue.	8.1	More Details
CVE-2026-42724	Unauthenticated Local File Inclusion in CleanSkin <= 1.5.0 versions.	8.1	More Details
CVE-2026-42777	Unauthenticated Local File Inclusion in Aalto <= 1.8 versions.	8.1	More Details
CVE-2026-48193	Unauthenticated Local File Inclusion in Uminex <= 1.0.9 versions.	8.1	More Details
CVE-2026-	Unauthenticated Local File Inclusion in DukaMarket <= 1.3.0 versions.	8.1	More

48194			Details
CVE-2026-62020	Unauthenticated Local File Inclusion in TouchUp < 1.4 versions.	8.1	More Details
CVE-2026-39802	Unauthenticated Remote Code Execution (RCE) in Everest Backup <= 2.3.13 versions.	8.1	More Details
CVE-2026-66084	An authorization bypass vulnerability in Apache DolphinScheduler allows authenticated users to modify task definitions in projects they are not authorized to access through the /dolphinscheduler/projects/{projectCode}/task-definition/{code}/with-upstream endpoint. The endpoint fails to verify that the task definition identified by code belongs to the project specified by projectCode. An authenticated user can supply the code of a project they are authorized to access together with a task definition code from another project, bypassing project access restrictions and modifying the target task definition and its upstream dependencies. This vulnerability can compromise workflow integrity and disrupt task execution in unauthorized projects. This issue affects Apache DolphinScheduler: before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	8.1	More Details
CVE-2026-92975	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.8.3 via the `create_support_user()` function. This is due to the function identifying the support account solely by matching against publicly hardcoded constants — `user_login` `groundhogg` and email addresses `support@groundhogg.io` / `help@groundhogg.io` — where the `in_array()` email-equality check at line 238 is not a security boundary because any user fully controls their own email value. This makes it possible for an attacker with an account whose `user_login` is `groundhogg` and whose `user_email` matches one of the hardcoded support constants to have that account silently promoted to administrator — and additionally to super admin on multisite when the triggering administrator holds `manage_network_options` — resulting in full site takeover. Exploitation requires a two-actor flow: the attacker must first obtain or pre-plant an account with the hardcoded credentials (possible when open user registration is enabled or another account-creation path exists), after which a legitimate administrator must invoke the support-access feature via the `submit_ticket` or `process_send_support_access` entry points to trigger the promotion.	8.1	More Details
CVE-2026-82895	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	8.1	More Details
CVE-2026-62376	Vikunja is an open-source self-hosted task management platform. Versions prior to 2.4.0 store password-reset, email-confirmation, and account-deletion tokens in the `user_tokens` table in plaintext. If an attacker gains read access to the database through a backup leak, misconfigured storage, or SQL-level exposure, they can immediately use pending tokens to take over user accounts without knowing passwords. Version 2.4.0 fixes the issue.	8.1	More Details
CVE-2026-84058	IBM Guardium Data Protection 12.0, 12.1, and 12.2 is vulnerable to a buffer overrun in the TDS (Microsoft SQL Server) PRELOGIN packet decoder. A remote attacker who can send a specially crafted TDS PRELOGIN packet to a network monitored by an IBM Guardium Collector may cause a denial of service or potentially execute arbitrary code on the Collector appliance.	8.1	More Details
CVE-2026-108853	UnicomAI Wanwu before 0.6.3 contains an insecure direct object reference vulnerability that allows authenticated low-privileged users to delete other tenants' agent or RAG applications by supplying their appld. Attackers can send requests to DELETE /v1/appspace/app with guessed sequential assistant IDs to permanently delete victims' applications, workflows, conversations, and associated data.	8.1	More Details
CVE-2026-15784	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.	8.1	More Details
CVE-2026-105411	An Authorization Bypass Through User-Controlled Key vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker with tracker administration rights on one tracker to update or delete fields of all the trackers on the instance.	8.1	More Details
CVE-2026-82334	IBM Guardium Data Protection 12.0, 12.1, 12.2 is vulnerable to a heap-based out-of-bounds read in the TDS7 LOGIN7 protocol parser. A remote attacker could send a specially crafted TDS LOGIN7 packet containing invalid offset or length values, potentially causing information disclosure or denial of service.	8.1	More Details
CVE-2026-14497	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote authenticated attacker to bypass security restrictions due to improper verification of cryptographic signatures.	8.1	More Details
CVE-	pH7Builder (pH7 Social Dating CMS) before 18.5.0 contains a path traversal vulnerability in the picture module deletePhoto() action that allows authenticated members to delete arbitrary files. Attackers can		More

2026-108902	supply ../ sequences in the POST picture_link parameter to remove other members' photos or configuration and cache files, causing content loss and denial of service.	8.1	Details
CVE-2026-82335	IBM Guardium Data Protection 12.0, 12.1, 12.2 is vulnerable to a heap-based buffer overflow in the MongoDB protocol parser. A remote attacker could send a specially crafted MongoDB SCRAM username containing an excessive length and cause memory corruption, potentially resulting in denial of service or arbitrary code execution.	8.1	More Details
CVE-2026-82344	IBM Guardium Data Protection 12.0, 12.1 is vulnerable to a heap-based buffer overflow in the S-TAP TrafficTap TDS login reassembly functionality. An unauthenticated remote attacker can send crafted TDS login fragments that exceed the fixed-size reassembly buffer, potentially resulting in denial of service or arbitrary code execution on the affected system.	8.1	More Details
CVE-2026-59347	VMware Workstation and Fusion contain a stack-based buffer-overflow vulnerability in HGFS. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. Affected versions: - VMware Workstation: 25H2, 26H1 (fixed in 26H1u1) - VMware Fusion: 25H2, 26H1 (fixed in 26H1u1)	8.1	More Details
CVE-2026-82900	IBM Guardium Data Protection 12.2.2, and 12.1 could allow a remote attacker to delete arbitrary files due to improper limitation of a pathname to a restricted directory.	8.1	More Details
CVE-2026-84035	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.	8.1	More Details
CVE-2026-108157	Pingvin Share X from 0.19.0 before 1.22.0 contains an improper authentication vulnerability that allows remote unauthenticated attackers to take over accounts by abusing automatic OAuth email linking in OAuthService.signUp(). Attackers can register a victim's unverified email on an enabled OAuth/OIDC provider, exploiting the missing email_verified check in GenericOidcProvider, to sign in as the victim including administrators while bypassing TOTP.	8.1	More Details
CVE-2026-19186	ieee802154_decipher_data_frame() in subsys/net/l2/ieee802154/ieee802154_frame.c computed payload_len = net_pkt_get_len(pkt) - ll_hdr_len - authtag_len without first checking that the received frame is at least ll_hdr_len + authtag_len bytes long. All three variables are uint8_t, so a frame whose payload is shorter than the configured authentication tag makes the subtraction wrap around to a large value (up to 255). The wrapped length is passed unchanged to ieee802154_decrypt_auth() and on to the CCM operation as cipher_pkt.in_len/out_buf_max, with apkt->tag pointing at frame + ll_hdr_len + payload_len. Because the receive buffer is allocated to the exact length of the frame received from the radio driver, the crypto layer then reads several hundred bytes past the end of the packet buffer and writes the same number of decrypted bytes back over it in place. The frame's authentication tag is only verified after this processing has taken place, so no key material, association or prior authentication is needed — a single crafted short frame from any device in radio range is sufficient. Frame validation in ieee802154_validate_frame() does not prevent it: a data frame is accepted with a one-byte payload. The result is an out-of-bounds read and an out-of-bounds write of up to roughly 240 bytes into the adjacent network-buffer pool, corrupting other packets or allocator metadata and typically faulting the target. The out-of-bounds content is not attacker-chosen (it is ciphertext XOR keystream over out-of-bounds memory) and the frame is dropped when tag verification fails, so the primary impact is memory corruption and denial of service rather than information disclosure. Exposure is limited to configurations that enable the experimental CONFIG_NET_L2_IEEE802154_SECURITY option, select a crypto device via CONFIG_NET_L2_IEEE802154_SECURITY_CRYPTODEV_NAME, and have established a security session with a level other than IEEE802154_SECURITY_LEVEL_NONE; with security disabled or at level NONE the tag length is zero and no underflow occurs. The fix rejects frames shorter than ll_hdr_len + authtag_len before the subtraction, and adds the matching guard on the transmit side in ieee802154_create_data_frame().	8.1	More Details
CVE-2026-84057	IBM Guardium Data Protection 12.2.2, and 12.1 could allow a remote attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	8.1	More Details
CVE-2026-84247	IBM Guardium Data Protection 12.2 could allow a remote authenticated attacker to cause a denial of service due to a path traversal vulnerability.	8.1	More Details
CVE-2026-84246	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	8.1	More Details
CVE-2026-107810	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, internal/backup/restore.go extracts inner archives before applying the restore_nginx and restore_nginx_ui flags and permits symlinks targeting the live Nginx configuration path. An authenticated user who can create and restore backups can craft a valid backup that places a symlink in the staging tree and then writes a regular file through that link, even when both restore flags are false. This can persistently inject configuration or cause denial of service	8.1	More Details

	when the modified files are later consumed. This issue is fixed in version 2.5.0.		
CVE-2026-107808	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, POST /api/login checks EnabledOTP but does not require a WebAuthn assertion when EnabledPasskey is true and no TOTP secret is configured. A passkey-only account is therefore issued a session after password verification, despite Enabled2FA reporting that the account has a second factor. An attacker who obtains the password can take over the account and reach administrative functionality without the registered passkey. This issue is fixed in version 2.5.0.	8.1	More Details
CVE-2026-84209	IBM Guardium Data Protection 12.2.2, and 12.1 could allow a remote attacker to execute arbitrary SQL commands due to improper neutralization of special elements used in an SQL command.	8.1	More Details
CVE-2026-19494	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to bypass security restrictions due to improper authentication.	8.1	More Details
CVE-2026-57458	Vikunja is an open-source self-hosted task management platform. In version 2.3.0, a scoped API token limited to the `oauth.authorize` permission can call `POST /api/v1/oauth/authorize`, obtain an OAuth authorization code, and exchange the code at `POST /api/v1/oauth/token` for a normal bearer JSON Web Token (JWT) and refresh token. The resulting credentials are not restricted by the original API token's permissions, allowing access to routes outside its declared scope for the same user. Version 2.4.0 fixes the vulnerability.	8.1	More Details
CVE-2026-39460	Username and passwords, including the default factory credentials, are stored in plaintext within the configuration file. With administrator rights, the configuration file can be viewed through the CLI or they can be exported from the device through a TFTP transfer from the web interface. A TFTP transfer can be initiated through SNMP which does not require authentication.	8.1	More Details
CVE-2026-62074	Unauthenticated Local File Inclusion in Ozeum <= 1.3.0 versions.	8.1	More Details
CVE-2026-46570	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in ntfs_index_walk_down() in libntfs-3g/index.c that allows an attacker to corrupt heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered by reading the special crafted file metadata.	8.1	More Details
CVE-2026-94062	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Fuelthemes Werkstatt werkstatt allows PHP Local File Inclusion. This issue affects Werkstatt: from n/a through 4.8.3.	8.1	More Details
CVE-2026-103360	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	8.1	More Details
CVE-2026-104899	The GeoDirectory - WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.8.187 via the 'design_type' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. The required nonce is trivially obtainable by any anonymous visitor, as the geodir_basic_nonce value is localized to every public frontend page via the geodir_params script object, meaning no authentication, user interaction, or specific site content is required to exploit this vulnerability.	8.1	More Details
CVE-2026-93445	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code.	8.1	More Details
CVE-2026-107910	An improper authentication vulnerability in the is_authenticated function (src/bolt/bolt_api.c) in FalkorDB before 4.20.0 allows a remote unauthenticated attacker to execute graph queries without credentials through the Bolt endpoint. The function decides whether a password is required by issuing an empty AUTH command to Redis and treats only a WRONGPASS error as meaning that a password is required; any other error, such as LOADING while a dataset is being loaded, MASTERDOWN during replication failover, or OOM under memory pressure, causes the client to be treated as authenticated. Only deployments that enable the Bolt endpoint (BOLT_PORT, disabled by default) are affected.	8.1	More Details
CVE-2026-7827	A stack-based buffer overflow in the _RdbLoadEntity function of the RDB graph decoders (src/serializers/decoders/*/decode_graph_entities.c) in FalkorDB before 4.18.4 allows a remote attacker who can issue Redis replication commands (for example, against an instance with no password configured) to cause a denial of service and possibly execute arbitrary code by supplying a crafted RDB stream with an attacker-controlled entity property count. The count sizes two variable-length arrays on the thread stack with no upper bound, and the decoder then fills them with attacker-supplied values.	8.1	More Details

CVE-2026-94067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Fuelthemes The Voux thevoux-wp allows PHP Local File Inclusion.This issue affects The Voux: from n/a through 6.9.5.	8.1	More Details
CVE-2026-107183	llama.cpp before b11393 contains a use-after-free and double free vulnerability in common_chat_peg_mapper::map that allows unauthenticated remote attackers to corrupt heap memory via a dangling current_tool pointer. Attackers can submit a chat_parser in a POST /completion request emitting a tool-id after a tool-close tag to crash llama-server and shape a heap write primitive.	8.1	More Details
CVE-2026-106471	A flaw was found in Candlepin. The central authorization filter incorrectly grants access when any one of multiple @Verify-annotated parameters is accessible, instead of requiring access to every verified entity. A low-privilege authenticated attacker who can access the first referenced object can bypass authorization checks on subsequent objects. When target resource identifiers are known, this can enable unauthorized disclosure of consumer information and unauthorized modification of entitlements and related subscription resources, including across organizations.	8.1	More Details
CVE-2026-107181	Telegram Desktop before 7.2.9 contains an IPC record-separator injection vulnerability in Core::Sandbox that allows remote attackers to inject OPEN: records via crafted tg:// links containing unescaped semicolons. Attackers can reach the interpret: scheme handler to upload local files, including tdata session keys, to an attacker channel, enabling account takeover.	8.1	More Details
CVE-2026-33367	SNMP can be used to perform administrative actions such as retrieving configuration files, modifying user accounts or device settings, and initiating firmware or bootloader upgrades or downgrades—all without any authentication.	8.1	More Details
CVE-2026-108718	Rill 0.77.0 through 0.90.5 contains a missing authorization vulnerability in the admin OAuth server that issues authorization codes to dynamically registered clients without user consent. Attackers can register a client with the long_lived_access_token scope and lure a user to an authorization link, obtaining a non-expiring API token with the user's full permissions.	8.1	More Details
CVE-2026-97674	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary OS commands due to improper neutralization of special elements used in an OS command ('Code Injection'), aka improper control of code generation.	8.1	More Details
CVE-2026-107723	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.3.0, fast-jwt createVerifier accepts a validly signed JWT whose payload is a JSON array because src/decoder.js checks that the payload is an object but does not reject arrays. The claim validator loop then finds no named exp, nbf, iss, aud, sub, jti, or nonce properties and silently skips those configured checks, returning the array as a successfully verified payload. An attacker who can produce or influence a validly signed token may bypass expiry, issuer, audience, subject, revocation, and replay protections. The opt-in requiredClaims option can block missing claims, and signature verification itself is not bypassed. This issue is fixed in version 6.3.0.	8.1	More Details
CVE-2026-14888	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to execute arbitrary code due to a heap-based buffer overflow.	8.1	More Details
CVE-2026-104797	The Advanced Form Integration — Connect Forms to 300+ Apps plugin for WordPress is vulnerable to Authentication Bypass via Unverified Password Change in all versions up to, and including, 2.9.0 The `adfoin_ultimatememberac_send_data` function, which powers the Ultimate Member "Update Profile Field" action, resolves the target WordPress user from an attacker-supplied email address and passes an attacker-controlled field key and value directly to `UM()->user()->update_profile()` in the `account` context — which explicitly bypasses Ultimate Member's banned-key validation — without performing any submitter identity verification, ownership check, capability check, current-password reauthentication, or restriction on sensitive keys such as `user_pass`. This makes it possible for unauthenticated attackers to change the password of any WordPress user account, including Administrator accounts, by submitting a public Contact Form 7 form with a target email and `user_pass` as the field key, enabling full site takeover. Exploitation requires an administrator to have pre-configured a Contact Form 7 integration that maps the target email, field key, and value from public form inputs to the Ultimate Member Update Profile Field action — the exact workflow the plugin's own UI advertises for this action type.	8.1	More Details
CVE-2026-84198	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	8.1	More Details
CVE-2026-104081	KodExplorer before 4.55 contains a path traversal vulnerability in the unzip_pre_name() function within app/function/helper.function.php, where a single non-recursive str_replace() sanitization pass can be bypassed using crafted filenames like "...//", combined with PclZip's extract() call in KodArchive.class.php lacking the PCLZIP_OPT_EXTRACT_DIR_RESTRICTION option. Authenticated attackers can upload a malicious ZIP archive with traversal sequences to overwrite arbitrary files such as core JavaScript assets, enabling stored XSS that leads to admin account takeover and subsequent remote code execution via unrestricted PHP file upload.	8.1	More Details

CVE-2026-66087	An authorization bypass vulnerability in Apache DolphinScheduler allows authenticated users to operate task instance in projects they are not authorized to access through the <code>*/dolphinscheduler/projects/{projectCode}/task-instances/{taskInstanceId}/stop</code> and <code>*/dolphinscheduler/projects/{projectCode}/task-instances/{taskInstanceId}/savepoint</code> . This issue affects Apache DolphinScheduler: before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	8.1	More Details
CVE-2026-105816	Vault and Vault Enterprise did not consistently verify that stored plugin catalog entries reference binaries within the configured plugin directory. When Vault uses Shamir seals and has an external plugin directory configured, a privileged operator able to restore an Integrated Storage (Raft) snapshot may be able to execute arbitrary code on the Vault host. This vulnerability (CVE-2026-105816) is fixed in Vault Community Edition 2.1.2, and Vault Enterprise 2.1.2, 1.21.12, 1.20.17, and 1.19.23.	8.0	More Details
CVE-2026-15781	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote authenticated attacker to execute arbitrary code due to a buffer overflow.	8.0	More Details
CVE-2026-87761	The Advised Web Push Notification WordPress plugin through 2.5.7 does not perform any capability or nonce check before allowing an authenticated user to overwrite its site-wide configuration, and does not escape those configuration values before printing them inside an inline script block on every front-end page, allowing any authenticated user, such as a subscriber, to perform Stored Cross-Site Scripting attacks against every visitor, including administrators.	8.0	More Details
CVE-2026-103647	Cross-site scripting in the webmail of Progressive Robot hMailServer 6.3.2 through 6.3.5 allows a remote attacker who can send a user an encrypted message to run script in the webmail's origin with that user's session. When the webmail decrypted an S/MIME message (from 6.3.2) or an OpenPGP message (from 6.3.4) in the browser, it offered each decrypted attachment as a blob URL of the media type the message declared for it. A click saved the file, but if the user opened the attachment in a new tab, a part declared as text/html was rendered as a document of the webmail's origin and its script could read the mailbox, send mail and change the account through the REST API. The webmail is served only when the REST API is enabled, which it is not by default.	8.0	More Details
CVE-2026-107821	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, MariaDB insufficiently validated counts, offsets, lengths, and field boundaries in FRM metadata while opening binary FRM files. An attacker able to place a crafted FRM file in the data directory could trigger out-of-bounds reads or writes, crash the server, or potentially execute code. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	8.0	More Details
CVE-2026-107615	An uncontrolled search path element vulnerability in GlavSoft TightVNC Server for Windows before 2.8.88 allows a local authenticated user to execute arbitrary code with SYSTEM privileges. <code>DynamicLibrary::init()</code> (and <code>ThemeLib</code>) load <code>screenhooks32.dll</code> / <code>screenhooks64.dll</code> with <code>LoadLibrary()</code> using a bare file name and no <code>LOAD_LIBRARY_SEARCH_*</code> flags, so the TightVNC service follows the default DLL search order and loads an attacker-planted DLL from a writable directory earlier in that order (for example, an installation directory with permissive ACLs).	7.8	More Details
CVE-2026-108953	mac-shell-mcp before 2.0.0 contains an OS command injection vulnerability that allows MCP clients to bypass the command whitelist by injecting shell metacharacters into <code>execute_command</code> arguments. Attackers or malicious prompts can call a safe command such as <code>pwd</code> with arguments like <code>;'</code> to run forbidden commands as the server user without approval.	7.8	More Details
CVE-2026-107612	Incorrect permission assignment in GlavSoft TightVNC Server for Windows before 2.8.88 allows a local authenticated user to read or overwrite the inter-process communication handles used between the TightVNC service and its desktop server process. The named shared memory segment in the <code>Global\</code> namespace that carries the pipe <code>HANDLE</code> values is created with a <code>NULL</code> DACL, and its name is derived from a time-seeded <code>srand(time(0))</code> value that is predictable to one-second granularity. A low-privileged local process can open the mapping and tamper with the IPC channel of a service running as <code>SYSTEM</code> , potentially leading to disclosure of session data, privilege escalation, or denial of service.	7.8	More Details
CVE-2026-19575	The user-mode verification handler for the <code>device_deinit()</code> system call, <code>z_vrfy_device_deinit()</code> in <code>kernel/device.c</code> , validated its <code>dev</code> argument with <code>K_SYSCALL_OBJ_INIT(dev, K_OBJ_ANY)</code> . <code>k_object_validate()</code> short-circuits its type comparison when the requested type is <code>K_OBJ_ANY</code> , so the check reduced to "this pointer is the base address of some kernel object the calling thread has been granted" — the object's actual type was never compared, and <code>K_SYSCALL_OBJ_INIT</code> also skips the initialization-state check. The sibling handlers <code>z_vrfy_device_init()</code> and <code>z_vrfy_device_is_ready()</code> already used <code>K_OBJ_DRIVER_ANY</code> and were unaffected. A thread running in user mode can therefore pass any kernel object it holds permission on — most usefully a thread stack object obtained from the <code>k_thread_stack_alloc()</code> syscall or a statically defined <code>K_THREAD_STACK</code> it was granted in order to spawn a child user thread — whose backing memory is writable from user mode. <code>z_impl_device_deinit()</code> then interprets those attacker-written bytes as a struct <code>device</code> : it dereferences the state pointer read out of the object, calls the function pointer read out of <code>ops.deinit</code> , and on success writes through state again. The result is an indirect call to an arbitrary address executed in supervisor mode, plus an arbitrary kernel read and a single-byte kernel write. Exploitation gives a local unprivileged thread full kernel code execution, defeating the <code>CONFIG_USERSPACE</code> isolation boundary entirely;	7.8	More Details

	a less precise attempt yields a supervisor-mode fault and a system crash. The defect is only reachable in builds that enable both CONFIG_USERSPACE and CONFIG_DEVICE_DEINIT_SUPPORT — with de-initialization support disabled, <code>z_impl_device_deinit()</code> returns <code>-ENOTSUP</code> without ever dereferencing the pointer. In v4.2.x and v4.3.x, CONFIG_DEVICE_DEINIT_SUPPORT defaulted to <code>y</code>, so every CONFIG_USERSPACE build of those releases is exposed unless the option was explicitly turned off. From v4.4.0 the option is opt-in (no default, and not selected by any in-tree subsystem), so a v4.4.x build is exposed only if it enables the option explicitly. The v4.2 line is no longer maintained and receives no backport. The fix changes the object check to <code>K_OBJ_DRIVER_ANY</code>, which constrains the argument to the build-generated driver object type range (<code>K_OBJ_DRIVER_FIRST..K_OBJ_DRIVER_LAST</code>) — the real struct device instances placed by the linker — so the state and <code>ops.deinit</code> fields are once again kernel-controlled.		
CVE-2026-11318	Deskin through 3.3.4.3 contains a privilege escalation vulnerability in the <code>com.deskin.service.installer</code> XPC service that allows local unprivileged attackers to execute arbitrary installer packages as root by connecting to the root-owned service without authentication. Attackers can invoke the privileged installer method to run an attacker-supplied installer, achieving full root compromise of the macOS host.	7.8	More Details
CVE-2026-102256	Post-authentication Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability has been identified in the SMA1000 appliance which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands, resulting in remote code execution.	7.8	More Details
CVE-2026-107914	Backdrop CMS 1.34 before 1.34.5 and 1.35 before 1.35.1 doesn't sufficiently protect configuration exports when delivering a compressed archive. This vulnerability is mitigated by the fact that an export must have been previously requested by someone with the "Synchronize, import, and export configuration" permission. NOTE: CVE-2026-107914 refers to the vulnerability in which <code>config.admin.inc</code> does not ensure that a <code>file_unmanaged_delete</code> operation occurs. Therefore, many archives could persist: <code>config.tar.gz</code>, <code>config_0.tar.gz</code>, <code>config_1.tar.gz</code>, etc. There is a separate <code>config.module</code> issue that could allow remote access by an anonymous user, but only for the one filename <code>config.tar.gz</code>.	7.8	More Details
CVE-2026-104077	Obsidian Desktop before 1.14.0 contains a remote code execution vulnerability that allows attackers to craft malicious Markdown notes exploiting insufficient sanitization of the <code>data-background-iframe</code> attribute, which bypasses <code>DOMPurify</code> and is processed by the bundled <code>Reveal.js</code> 4.3.1 within the <code>Slides</code> core plugin, allowing a <code>javascript: URL</code> to execute in the resulting background iframe. Because Node integration is enabled and context isolation is disabled in Obsidian's vault renderer, the injected script can call <code>parent.require()</code> to access Node APIs such as <code>fs</code> and <code>child_process</code>, enabling arbitrary operating system command execution when the victim opens the note and manually starts the presentation.	7.8	More Details
CVE-2026-104078	Obsidian Desktop before 1.14.0 contains a filter bypass vulnerability in the bundled <code>MathJax</code> 3.2.2 <code>Safe</code> component that allows attackers to execute arbitrary code by embedding a crafted <code>\href</code> value with a <code>TAB</code> byte in the URL scheme, causing <code>filterURL</code> to produce an empty protocol that bypasses the configured <code>safeProtocols</code> restrictions. Attackers can craft a note containing a malicious <code>MathJax</code> formula that renders as a <code>javascript: URL</code> anchor, which when clicked by the victim in <code>Live Preview</code> executes in the <code>Node-integration-enabled</code> vault renderer via <code>require('child_process')</code>, achieving arbitrary operating system command execution as the desktop user.	7.8	More Details
CVE-2026-42616	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in <code>cat()</code> in <code>ntfscat.c</code> that allows an attacker to corrupt heap memory in the <code>ntfscat</code> binary by crafting a malicious NTFS image. The overflow is triggered by reading a file.	7.8	More Details
CVE-2026-103010	Heap-based buffer overflow in the legacy Blowfish decryption routine (<code>BlowFishEncryptor::DecryptFromString</code>) in Progressive Robot <code>hMailServer</code> 6.0.0 through 6.3.3 on Windows allows a local interactive user with no <code>hMailServer</code> credentials to write bytes of their choosing past the end of a 255-byte heap buffer in the <code>hMailServer</code> service process, which runs as <code>LocalSystem</code> by default. The user does this by passing a long hexadecimal string to the <code>COM</code> method <code>Utilities.BlowfishDecrypt</code>, which checked no authentication. The routine converted hexadecimal input of any length into a fixed 255-byte buffer before decrypting it in place. The result is a denial of service (service crash), and possibly code execution with the privileges of the service account.	7.8	More Details
CVE-2026-107322	An incomplete list of disallowed inputs in Amazon Agent Plugins for AWS databases-on-aws plugin before 1.7.1 might allow a remote unauthenticated actor to execute arbitrary operating system commands on the host running the helper via a crafted database command value introduced in the agent context. To remediate this issue, users should upgrade to <code>databases-on-aws</code> plugin version 1.7.1 or later and verify that the updated plugin is active in each environment where it is used.	7.8	More Details
CVE-2026-104658	The Linux live-update apply helper (<code>hmailserver-update</code>) of Progressive Robot <code>hMailServer</code> 6.3.4 and 6.3.5 runs as root on a request file written by the unprivileged <code>hmailserver</code> service account, and took from that request the program used to verify an <code>Applmage</code> update's signature and the <code>systemd</code> unit to stop before reading the service account's files. An attacker who already runs code as the <code>hmailserver</code> service account, for example through another flaw in the mail server, can therefore have arbitrary code executed as root, on any Linux installation where the live update's path unit is active - the default for the project's <code>.deb</code> and <code>.rpm</code> packages - and on <code>Applmage</code> installations run under that unit.	7.8	More Details

CVE-2026-104660	Missing authorization on COM objects in Progressive Robot hMailServer 6.0.0 through 6.3.5 (Windows only) lets a local interactive user with no hMailServer credential read and write arbitrary files as the service account and queue mail as any sender. The service registers its COM classes with no DCOM access or launch permission and calls CoInitializeSecurity with no security descriptor, so any user logged on at the console or over Remote Desktop can activate the classes in the running service; a hMailServer.Message, its Attachments and Attachment, and a hMailServer.FetchAccount created this way carry a credential that never authenticated. Attachments.Add(path) and Attachment.SaveAs(path) performed no authorization check, and Message.Save/SaveCopy and FetchAccount.AccountID/Save performed none either up to 6.3.3 and from 6.3.4 treated a holder with no credential as the server's own event-script host. Because the service does not impersonate the COM caller, Attachments.Add reads any file the service account can read and returns it, Attachment.SaveAs writes attacker-chosen bytes to any path it can write (on a LocalSystem installation, code execution as SYSTEM), Message.Save queues outbound mail from any address past the SMTP checks, and FetchAccount attaches a mail-fetch job to any mailbox. The objects an Application handed out behave the same once a later Authenticate on that Application fails.	7.8	More Details
CVE-2026-92705	Aegisub is a cross-platform advanced subtitle editor. From 3.2.0 to 3.4.2, Aegisub automatically loads Automation scripts referenced by `Automation Scripts` metadata in `ASS` subtitle projects without asking whether the user trusts the scripts or their authors. An attacker can distribute a crafted `ASS` file together with a referenced malicious Automation script, and opening the `AS` file executes arbitrary code with the privileges of the Aegisub process. From 3.4.0 to 3.4.2, inconsistent handling of embedded `NUL` characters between extension validation and filesystem operations additionally allows a crafted `ASS/Lua` polyglot to reference and execute itself as a single-file variant. The vulnerability is fixed in Aegisub 3.5.0.	7.8	More Details
CVE-2026-107782	System Informer before 4.0.26241.138 contains an incorrect authorization vulnerability in the phsvc helper that allows local attackers to reach privileged APIs by connecting from any Authenticode-signed process. Attackers can load code into a Microsoft-signed host like rundll32.exe, connect to SiSvcApiPort, and call PhSvcApiCreateService to execute code as SYSTEM.	7.8	More Details
CVE-2026-107707	Intego Antivirus for Windows through 3.0.0.1 contains a link following vulnerability in its optimization module that allows local unprivileged users to delete arbitrary folders as SYSTEM. Attackers can replace a scanned duplicate file's directory with a junction to C:\Config.msi and abuse Windows Installer rollback to execute code as SYSTEM.	7.8	More Details
CVE-2026-106057	patool before 4.0.6 contains an OS command injection vulnerability on Windows because shell_quote_nt fails to escape cmd.exe metacharacters or embedded double quotes in archive filenames. Attackers can supply crafted filenames like report&calc.gz for single-file formats run with shell=True to execute commands with patool process privileges.	7.8	More Details
CVE-2026-107573	Incorrect default permissions in the Windows installer of Progressive Robot hMailServer 6.0.0 through 6.3.5 allow a local authenticated user to read the mail server's data. The installer created the data, log, temp, database and event folders and the hMailServer.INI configuration file with the permissions inherited from the installation folder, by default under Program Files, which give the local Users group read access. Any user who can sign in to the computer could read every stored message, the logs, the built-in database with the accounts' password hashes whenever the service is stopped, and the configuration file, including the database password, which is sealed only with the machine's DPAPI key and can be unsealed by any local account; with an external database that password gives full control of it. The Linux Applmage of 6.3.0 through 6.3.5 likewise created its per-user data folders readable by other local users.	7.8	More Details
CVE-2026-84245	IBM Guardium Data Protection 12.2 is vulnerable to a local privilege escalation in the cp_wrapper component. A low-privileged local user could exploit this vulnerability to gain root privileges and access or modify sensitive system files.	7.8	More Details
CVE-2026-19669	The user-mode syscall verifiers z_vrfy_fuel_gauge_get_props() and z_vrfy_fuel_gauge_set_props() in drivers/fuel_gauge/fuel_gauge_syscall_handlers.c declared two variable-length arrays, union fuel_gauge_prop_val k_vals[len] and fuel_gauge_prop_t k_props[len], sized directly by the caller-supplied len argument. len is an unvalidated size_t taken straight from the syscall ABI, and the VLAs were allocated before any check at all — including before the K_SYSCALL_DRIVER_FUEL_GAUGE() object-permission check. The subsequent k_usermode_from_copy() calls validated only that the user source buffer was readable; the kernel destination was never bounds-checked, since it was sized by the same attacker-chosen len. Any thread running in user mode with CONFIG_USERSPACE enabled can invoke fuel_gauge_get_props() or fuel_gauge_set_props() with a large len. This first displaces the supervisor stack pointer by an arbitrary attacker-chosen amount — Zephyr does not build with stack-clash probing, so the displacement itself does not fault, and the nested calls made by the verifier then write frames below the privileged stack. If the caller has been granted access to a fuel-gauge device object, the memcpy inside k_usermode_from_copy() additionally writes len * sizeof(union fuel_gauge_prop_val) bytes of fully attacker-controlled data starting well below the stack base. CONFIG_PRIVILEGED_STACK_SIZE defaults to 1024 bytes, so a len of roughly 170 already exhausts it. The result is an out-of-bounds write in supervisor mode with attacker-controlled length and, on the permitted path, attacker-controlled content — a break out of the user-mode sandbox into kernel memory, leading to kernel code execution or a system crash. A stack guard region does not contain it, because the copy begins below the guard and walks upward, corrupting unprotected memory before the guard is reached. The fix removes the kernel-side copies entirely and validates the caller's arrays in place	7.8	More Details

	with K_SYSCALL_MEMORY_ARRAY_READ() / K_SYSCALL_MEMORY_ARRAY_WRITE(), which also handle the len * size multiplication overflow; this is safe because neither fuel_gauge_prop_t nor union fuel_gauge_prop_val contains embedded pointers.		
CVE-2026-19736	The NXP MCUX TRNG entropy driver in drivers/entropy/entropy_mcux_trng.c passed the caller's byte count straight to the vendor SDK routine TRNG_GetRandomData(). On i.MX RT5xx and RT6xx parts the SDK compiles its TRNG_SW_HEALTH_TESTS variant, which always copies whole 32-bit words and draws entropy rounded up to a multiple of 128 bytes. Its "caller buffer is full" guard tests dataSize == 0, so a request whose length is not a multiple of four makes dataSize underflow past zero and the SDK keeps writing into the caller's buffer for the entire extraction: a 1-byte request results in 128 bytes written, and any non-word-multiple length overflows by up to 127 bytes. entropy_get_entropy() is a syscall, and its verifier in drivers/entropy/entropy_handlers.c validates only the requested length via K_SYSCALL_MEMORY_WRITE(). With CONFIG_USERSPACE enabled, an unprivileged user-mode thread that has merely been granted the entropy device can therefore choose both the destination address and a length such as 1, and cause the kernel to write up to 127 bytes beyond the region it proved it owns. On these Cortex-M33 targets there is no MMU, so user partitions and kernel data share one SRAM and the overflow can land in adjacent kernel state. The same defect is reached from kernel mode by any caller requesting a non-word-multiple length, including getentropy() and, in builds where sys_csrand_get()/sys_rand_get() resolve to the hardware generator, sys_rand8_get() and sys_rand16_get(). Impact is memory corruption of up to 127 bytes immediately following the supplied buffer — typically the caller's stack in kernel-mode use, or memory outside the caller's partition when driven through the syscall. The overflow offset is fully determined by the requested length and is therefore deterministic, while the written content is uncontrolled TRNG output; the practical consequences range from crashes and unpredictable state corruption to opportunistic escalation when kernel bookkeeping such as object permission bitmaps is overwritten. The affected devices are those where the MCUX SDK enables TRNG_SW_HEALTH_TESTS (MIMXRT595S, MIMXRT555S, MIMXRT533S, MIMXRT685S, MIMXRT633S), on which the TRNG is the zephyr,entropy chosen node; other SoCs using this driver take the SDK path that clamps the copy size and are unaffected. The fix routes any unaligned prefix and any sub-word tail through a local bounce word and hands the SDK only word-multiple sizes, so the SDK's word-granular writes can no longer pass the end of the caller's buffer.	7.8	More Details
CVE-2026-107709	A path traversal vulnerability exists in Bower decompress-zip through version 0.3.3. The vulnerability located in `lib/decompress-zip.js` improperly validates archive entry paths during ZIP extraction. A crafted ZIP archive containing entries that resolve to prefix-sibling directories can cause files to be written outside the intended extraction directory. Successful exploitation may allow arbitrary file overwrite, application compromise, or remote code execution depending on the target environment and writable sibling paths.	7.8	More Details
CVE-2026-84271	IBM Guardium Data Protection 12.2 is vulnerable to a signature verification bypass in the patch installer. An attacker with local access could exploit this vulnerability to execute arbitrary code with root privileges.	7.8	More Details
CVE-2026-108976	GNU Emacs before 31.2 (and TRAMP through 2.8.2) allows OS command injection via a filename because tramp-user-regexp has an incomplete list of disallowed inputs. NOTE: this issue exists because of an incomplete fix for CVE-2026-79992.	7.8	More Details
CVE-2026-14507	IBM DataPower Gateway 11.0.0.0 through 11.0.0.2 could allow a remote authenticated attacker to cause a denial of service due to improper memory allocation during key derivation.	7.7	More Details
CVE-2026-76266	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15 on Linux, a local user who can run commands as the user account running Splunk Enterprise could cause an affected Linux package upgrade to run attacker-controlled operating-system commands with root privileges. The vulnerability is possible because the Linux package maintainer script trusts existing Splunk Enterprise installation content when it performs upgrade operations with root privileges. The vulnerability requires an affected Linux package upgrade to occur after the local user modifies the installation. The local user should not be able to elevate privileges at will.	7.7	More Details
CVE-2026-93017	The `insights-operator-gather` ClusterRole grants the operator's service account read access to secrets in the core API group with no namespace or resourceNames restriction — therefore, access to every secret in every namespace in the cluster. Ref: https://github.com/openshift/insights-operator/blob/8f15e3157ff09f54ab22801f5b21da35a195cc6d/manifests/03-clusterrole.yaml#L368-L373 ``` - apiGroups: - "" resources: - secrets verbs: - get - list ``` By spawning a pod with the gather service account mounted, an attacker will be able to access any secret in any namespace. ``` spec: serviceAccountName:"gather" ```	7.7	More Details
CVE-2026-40805	Subscriber Arbitrary File Deletion in PeepSo <= 9.0.5.4 versions.	7.7	More Details
CVE-2026-107352	Missing authorization checks in Amazon Athena engine version 3 request handling could have allowed an authenticated user to read limited query metadata (AWS account identifiers and SQL statement text) from other AWS accounts. Query results, credentials, and Amazon S3 data were not affected. AWS remediated the issue on September 1, 2026, and has confirmed no customer metadata was accessed. No customer action is	7.7	More Details

	required.		
CVE-2026-105833	EspoCRM before 10.0.5 contains an insecure direct object reference vulnerability in PersonalAccount\Service that allows users with Email Account scope access to retrieve other users' IMAP passwords. Attackers who know a victim's Email Account record ID can request that record to steal stored IMAP credentials and access the victim's mailbox.	7.7	More Details
CVE-2026-83947	Missing authorization in Azure Event Grid allows an authorized attacker to perform spoofing over a network.	7.7	More Details
CVE-2026-101331	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to insufficiently protected credentials.	7.7	More Details
CVE-2026-106510	Backstage is an open framework for building developer portals. Prior to 1.14.6, the @backstage/plugin-techdocs-node package is affected by remote code execution via crafted markdown_extensions in techdocs mkdocs.yml. An authenticated user who can register catalog entities can provide a crafted mkdocs.yml causing arbitrary OS command execution on the TechDocs build host when the docs are built. This issue is fixed in versions 1.14.6 and 1.15.4.	7.7	More Details
CVE-2026-106556	Backstage is an open framework for building developer portals. Prior to 1.14.6, the @backstage/plugin-techdocs-node package is affected by configuration bypass in techdocs mkdocs.yml sanitization. Insufficient validation of MkDocs configuration during TechDocs generation could allow an authenticated user who can register or modify documentation sources to execute arbitrary commands in the build environment. Impact is limited to resources accessible to the TechDocs backend or build container. This issue is fixed in versions 1.14.6 and 1.15.4.	7.7	More Details
CVE-2026-78530	Subscriber Arbitrary File Deletion in FoodBakery <= 4.6 versions.	7.7	More Details
CVE-2026-106557	Backstage is an open framework for building developer portals. Prior to 1.14.6 and 1.15.4, the @backstage/plugin-techdocs-node package did not sufficiently validate TechDocs Markdown extension configuration. An authenticated user who can register or modify documentation sources may cause a TechDocs build to access resources outside the intended documentation boundary, potentially exposing backend-host data or internal network resources. This issue is fixed in versions 1.14.6 and 1.15.4 when pymdown-extensions 10.21.3 or later is also used, normally through mkdocs-techdocs-core 1.7.0 or later.	7.7	More Details
CVE-2026-93677	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to exposure of sensitive information to an unauthorized actor.	7.7	More Details
CVE-2026-78024	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Server-Side Request Forgery (SSRF) vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure, Protection mechanism bypass, Server-side request forgery, and Unauthorized access.	7.7	More Details
CVE-2026-46569	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in ntfs_ib_copy_tail(), in libntfs-3g/index.c, that allows an attacker to corrupt heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered by extending a directory, e.g., by creating a file.	7.7	More Details
CVE-2026-107295	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.34.0 until 1.107.4 and 2.28.0, the Agent.to_web() and clai web development chat endpoint has missing request content-type validation. A website visited by a developer can submit a browser-compatible request to a loopback-hosted chat server, causing the served agent to run and execute tools with the privileges and credentials of the local process; client-relayed approval decisions also leave requires_approval=True tools exposed. Binding to localhost does not prevent a browser page from reaching the loopback address. This issue is fixed in versions 1.107.4 and 2.28.0.	7.6	More Details
CVE-2026-42720	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sarah Giles Dynamic User Directory dynamic-user-directory allows Blind SQL Injection.This issue affects Dynamic User Directory: from n/a through 2.4.	7.6	More Details
CVE-2026-42710	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in 10Web Slider by 10Web slider-wd allows Blind SQL Injection.This issue affects Slider by 10Web: from n/a through 1.2.63.	7.6	More Details
CVE-2026-42708	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AF themes WP Post Author wp-post-author allows Blind SQL Injection.This issue affects WP Post Author: from n/a through 4.0.0.	7.6	More Details

CVE-2026-108260	Tina is a headless content management system. Prior to 0.2.1, the tina-markdown element in packages/@tinacms/web-components/src/tina-markdown.js assigns a rich-text node.url value directly to an anchor href without validating the URL scheme. A content author can store a link using a script-capable scheme, and a visitor who clicks the rendered link executes attacker-controlled script in the site's origin. The script can access same-origin application data and, when the visitor is an editor or administrator, may expose credentials stored by the TinaCMS admin on that origin. This issue is fixed in version 0.2.1.	7.6	More Details
CVE-2026-107303	JHipster is a development platform to quickly generate, develop, and deploy modern web applications and microservice architectures. Prior to generator-jhipster 9.4.0 and react-jhipster 1.1.0, generated applications can persist attacker-controlled Blob data and companion ContentType values, return them through generated REST endpoints, and pass them to the generated openFile helper in generators/client/generators/common/templates/src/main/webapp/app/shared/jhipster/data-utils.ts.ejs. The helper uses the returned ContentType as the browser Blob MIME type and opens an object URL, so a normal authenticated user with write access to a Blob-bearing entity can store active HTML or SVG content that may execute under the application origin when a privileged user opens it. Exploitability depends on the generated application's content security policy and target-browser Blob behavior. This issue is fixed in generator-jhipster 9.4.0 and react-jhipster 1.1.0.	7.6	More Details
CVE-2026-42717	Administrator SQL Injection in Leyka <= 3.32.3 versions.	7.6	More Details
CVE-2026-42722	Administrator SQL Injection in Frontend Admin by DynamiApps <= 3.29.13 versions.	7.6	More Details
CVE-2026-45440	Administrator SQL Injection in WP Ultimate CSV Importer <= 9.2 versions.	7.6	More Details
CVE-2026-76283	Protection Mechanism Failure. Splunk addressed multiple internally identified vulnerabilities in Splunk Enterprise versions 10.4.3, 10.2.7, 10.0.10, and 9.4.15. The vulnerabilities are grouped by Common Weakness Enumeration (CWE), with one Common Vulnerabilities and Exposures (CVE) identifier assigned to each group. See Details for more information.	7.6	More Details
CVE-2026-42721	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SERVIT Software Solutions affiliate-toolkit affiliate-toolkit-starter allows Blind SQL Injection.This issue affects affiliate-toolkit: from n/a through 3.9.1.	7.6	More Details
CVE-2026-42714	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Piggly Dev Pix por Piggly (para Woocommerce) pix-por-piggly allows Blind SQL Injection.This issue affects Pix por Piggly (para Woocommerce): from n/a through 2.1.2.	7.6	More Details
CVE-2026-105076	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Appsbd Vitepos vitepos-lite allows Blind SQL Injection.This issue affects Vitepos: from n/a through 3.6.1.	7.6	More Details
CVE-2026-42713	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Gopiplus Post title marquee scroll post-title-marquee-scroll allows Blind SQL Injection.This issue affects Post title marquee scroll: from n/a through 9.9.	7.6	More Details
CVE-2026-62033	Subscriber Settings Change in uListing <= 2.2.0 versions.	7.6	More Details
CVE-2026-93678	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization.	7.6	More Details
CVE-2026-40802	Subscriber Settings Change in Pubjet 5.4.8 => پابجٹ versions.	7.6	More Details
CVE-2026-108760	LlamaFarm through 0.0.34 contains an insecure default configuration that binds its unauthenticated FastAPI server to 0.0.0.0 on port 14345, while the If CLI silently discards HOST overrides. Network-adjacent attackers can call the project and dataset management API to read stored provider API keys, modify projects, trigger ingestion, and irreversibly delete projects.	7.6	More Details
CVE-2026-67693	An issue in gnutls v.3.8.13 allows an attacker to obtain sensitive information via failing to reject end-entity X.509 certificates that contain a contradictory combination of Key Usage (KU) and Extended Key Usage (EKU)	7.5	More Details

CVE-2026-16170	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to a heap buffer overflow.	7.5	More Details
CVE-2026-84276	IBM Guardium Data Protection 12.2.2 is affected by a denial-of-service vulnerability in the edge-controller. An unauthenticated remote attacker with network access to the edge-controller gRPC service can provide malformed task data that triggers an unchecked type assertion, causing the edge-controller process to terminate unexpectedly.	7.5	More Details
CVE-2026-16169	IBM DataPower Gateway 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to uncontrolled resource consumption.	7.5	More Details
CVE-2026-107227	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. From 2.2.0 until 3.0.14, WebSocket permessage-deflate decompression is unbounded when compression is enabled. The inbound pipeline aggregates compressed frames before WebSocketClientCompressionHandler inflates them, so webSocketMaxFrameSize and webSocketMaxBufferSize do not bound decompressed output. A malicious WebSocket peer can send a small compressed message that expands to a very large Netty buffer and exhausts JVM heap. This issue is fixed in version 3.0.14.	7.5	More Details
CVE-2026-16178	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to improper input validation.	7.5	More Details
CVE-2026-16176	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to improper validation of the length field during memory reallocation.	7.5	More Details
CVE-2026-96662	The Appointment Booking Plugin – LatePoint Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to generic SQL Injection via 'booking[service_id]' Parameter in all versions up to, and including, 5.7.2 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-2026-16167	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to improper bounds checking.	7.5	More Details
CVE-2026-75349	EIPStackGroup OpENer v2.3.0/master up to commit 76b95cf contains an out-of-bounds read vulnerability in Connection Manager request parsing. This allows a remote attacker to cause a denial of service.	7.5	More Details
CVE-2026-107812	Nginx UI is a web user interface for the Nginx web server. From 2.0.0 until 2.5.0, the self-upgrade mechanism validates a downloaded binary only with a same-origin digest obtained from the same upgrade mirror. A compromised mirror or network attacker able to alter both responses can supply a malicious executable and matching digest. An operator-triggered upgrade is required, and the application installs and runs the attacker-controlled code in the Nginx UI process context on the next upgrade. This issue is fixed in version 2.5.0.	7.5	More Details
CVE-2026-103309	The GPTTranslate WordPress plugin before 2.34.14 does not properly restrict who can store translations, and does not escape them when outputting them in translated pages, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks when server-side translations are enabled.	7.5	More Details
CVE-2026-78795	An issue in Netcore B11 Enterprise-level full Gigabit 9-port shop wireless router v1.3.241114.024540 and before allows a remote attacker to obtain sensitive information	7.5	More Details
CVE-2026-96461	Missing Authorization vulnerability in TMS Amelia ameliabooking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Amelia: from n/a through 2.4.10.	7.5	More Details
CVE-2026-16179	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow an attacker to cause a heap buffer underwrite and potentially crash the service.	7.5	More Details
CVE-2026-93746	The WebToffee WooCommerce PDF Invoices, Packing Slips, Delivery Notes & Shipping Labels plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 5.0.2 via the 'email' parameter of the guest print_document_from_the_mail_link handler dispatched from print_window() on init. This is due to the handler authorizing access to an order's printable documents when the attacker-supplied (base64-encoded) 'email' equals the order's billing email — a non-secret identifier — instead of requiring the WooCommerce order_key. This makes it possible for unauthenticated attackers, when the site is configured to allow guest access to documents ('wt_pklist_print_button_access_for' != 'logged_in'), to retrieve	7.5	More Details

	any other customer's invoice, packing slip, delivery note, dispatch label or shipping label — including customer name, billing/shipping address, phone number, purchased products, prices, taxes and invoice metadata — by knowing the target order ID and the associated billing email address.		
CVE-2026-75348	An out-of-bounds read vulnerability exists in EIPStackGroup OpENER v2.3 and master up to commit 76b95cf in the EtherNet/IP TCP SendRRData Common Packet Format parser. The issue occurs in CreateCommonPacketFormatStructure() when it parses recognized optional socket address information items of type 0x8000 or 0x8001 without first validating that the remaining CPF buffer contains the complete fixed sockaddr structure. This allows a remote attacker to cause a denial of service.	7.5	More Details
CVE-2026-95209	An issue in gnutls v3.8.13 causes legitimate CA certificates to be rejected, leading to a Denial of Service (DoS).	7.5	More Details
CVE-2026-44031	Uncontrolled recursion in DcmSequenceOfItems::read() and DcmItem::read() in the dcmdata library of OFFIS DCMTK 3.7.0 allows a remote, unauthenticated attacker to cause a denial of service (stack exhaustion and process crash) via a DICOM dataset containing deeply nested sequences (SQ elements). The dataset can be sent in a C-STORE request to storescp, dcmrecv, dcmqrscp, or any other DICOM service built on DCMTK, because the received dataset is parsed before any authentication takes place. Local tools such as dcmdump also crash when opening such a file. The issue is fixed in commit 885ff0f10372bd589b5f44cea974f28a3964cb0f, which adds a configurable sequence nesting depth limit (default 64).	7.5	More Details
CVE-2026-75346	An out-of-bounds read vulnerability exists in EIPStackGroup OpENER v2.3 and master through commit 76b95cf in the server-side CIP SetAttributeList service. This allows a remote attacker to cause a denial of service	7.5	More Details
CVE-2026-96336	Authentication Bypass by Spoofing vulnerability in WPMU DEV Forminator forminator allows Identity Spoofing.This issue affects Forminator: from n/a through 1.57.2.	7.5	More Details
CVE-2026-75345	OpENER v2.3.0 / commit 76b95cf contains an out-of-bounds read in the unconnected explicit messaging path. This allows a remote attacker to cause a denial of service.	7.5	More Details
CVE-2026-14854	The WooCommerce Bookings WordPress plugin before 3.11.0 does not limit a user-supplied value before using it to allocate memory in one of its unauthenticated AJAX actions, allowing unauthenticated attackers to exhaust server memory and cause a Denial of Service with a single request.	7.5	More Details
CVE-2026-95208	An issue in the ConfirmNameConstraints() function (wolfcrypt/src/asn.c) of wolfSSL v5.9.1 and v5.9.2 allows attackers to cause a Denial of Service (DoS) via providing crafted Certificate Authority certificates, leading to valid certificates without SAN to be incorrectly rejected by wolfSSL-based TLS clients.	7.5	More Details
CVE-2026-93950	Missing Authorization vulnerability in StylemixThemes Motors motors allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Motors: from n/a through 1.4.108.	7.5	More Details
CVE-2026-96333	Authentication Bypass by Spoofing vulnerability in Liquid Web / StellarWP GiveWP give allows Identity Spoofing.This issue affects GiveWP: from n/a through 4.16.8.1.	7.5	More Details
CVE-2026-16164	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to a buffer overflow.	7.5	More Details
CVE-2026-19493	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote attacker to perform an arbitrary file write due to path traversal.	7.5	More Details
CVE-2026-107911	A type confusion vulnerability in the _read_flags function (src/commands/cmd_dispatcher.c) in FalkorDB before 4.20.0 allows a remote authenticated attacker who can run GRAPH.QUERY to cause a denial of service and possibly disclose or corrupt memory. The function accepts a --bolt argument from any client and casts the following command argument, a Redis string object, to a Bolt client structure without checking its origin; the result-set code then dereferences pointers read from that object. The argument is parsed even when the Bolt endpoint is disabled, so default configurations are affected.	7.5	More Details
CVE-2026-97031	Multiple ECH outer extension references are not permitted under RFC 9849; previously, a client could send a well-crafted packet that could trigger memory exhaustion in the server process by specifying multiple references. We now reject these as malformed and curb the memory amplification vector as a result.	7.5	More Details
CVE-2026-75352	OpENER v2.3/commit 76b95cf, contains an integer underflow in the server-side EtherNet/IP ForwardOpen connection-path parser. This allows a remote attacker to cause a denial of service	7.5	More Details

CVE-2026-107576	Inefficient algorithmic complexity in the inbound DKIM and ARC signature verification of Progressive Robot hMailServer 6.0.0 through 6.3.5 allows a remote unauthenticated attacker to make the mail services unavailable by sending a message. Building the canonical header and choosing the header fields named in a signature's h= tag took time growing with the square of the message's header: the 'simple' canonicalisation prepended each continuation line of a folded field to the lines already gathered, and both canonicalisations searched the gathered fields from the bottom for each h= name and erased the match from the middle of the list. A message whose header holds very many fields, or a field folded over very many lines, with a DKIM-Signature the attacker signs for a domain they control, keeps a worker thread busy for tens of seconds per signature; up to ten signatures are evaluated per message by each of the DKIM and DMARC tests, on the threads that serve delivery and SMTP.	7.5	More Details
CVE-2026-107577	Inefficient algorithmic complexity and a non-terminating loop in the MIME processing of received messages in Progressive Robot hMailServer 6.0.0 through 6.3.5 allow a remote unauthenticated attacker to make the mail services unavailable by sending a message. Removing a MIME header parameter whose value is empty and directly followed by a semicolon (for example a Content-Disposition with 'filename=a.bat; filename=;') entered a loop that never terminates, holding a worker thread at full load until the server is restarted; this is reached when the attachment blocker renames a blocked attachment or a filename is set over the REST API. Separately, decoding a header field that holds many RFC 2047 encoded words of an encoding other than base64 or quoted-printable, removing a parameter with many RFC 2231 continuations, and deleting many header fields of one name each took time growing with the square of the message, on the small thread pools that serve IMAP, SMTP and POP3 connections, delivery and the REST API.	7.5	More Details
CVE-2026-108863	Katanemo Plano through 0.4.37 contains a missing authentication vulnerability that allows unauthenticated network attackers to access the Envoy admin interface, which is bound to all host interfaces on port 9901. Attackers can request the /config_dump endpoint to read configured LLM provider API keys in plaintext from the WASM filter configuration.	7.5	More Details
CVE-2026-107579	Inefficient algorithmic complexity in the bounce and complaint processing of Progressive Robot hMailServer 6.3.4 and 6.3.5 allows a remote unauthenticated attacker to stop mail delivery by sending messages, when bounce processing or complaint processing is enabled or a mailing list is managed by the server (none is by default). The readers of incoming delivery status notifications (RFC 3464) and abuse feedback reports (RFC 5965) removed the blank lines at the start of the returned headers part two bytes at a time, copying the rest of the part each time, so their work grew with the square of the number of blank lines. A message shaped like such a report, whose headers part begins with a very large number of blank lines within the reader's 2 MB limit, keeps a delivery thread busy for over a minute while it is delivered, and a few such messages a minute keep every delivery thread busy.	7.5	More Details
CVE-2026-75351	OpENER v2.3/commit 76b95cf, contains an out-of-bounds read in the server-side EtherNet/IP ForwardOpen connection-path parser. This allows a remote attacker to cause a denial of service.	7.5	More Details
CVE-2026-75350	EIPStackGroup OpENER v2.3 / master commit 76b95cf contains a buffer overflow in the GetAttributeList() implementation for the EtherNet/IP Get_Attribute_List service. This allows a remote attacker to cause a denial of service	7.5	More Details
CVE-2026-107840	yopass is a service for securely sharing secrets, passwords, and files. Prior to version 14.7.0, the Prometheus metrics middleware in pkg/server/server.go uses the attacker-controlled r.Method value directly as the method label for yopass_http_requests_total and yopass_http_request_duration_seconds. Because the catch-all route accepts arbitrary HTTP method tokens, an unauthenticated remote attacker can submit many unique methods and create metric series that the Prometheus registry never evicts. The resulting monotonic memory growth can OOM-kill the process, while the expanding registry also degrades /metrics scrape latency and can blind monitoring. This issue is fixed in version 14.7.0.	7.5	More Details
CVE-2026-107839	ageLANServer provides a cross-platform web server and launcher for offline multiplayer in several Age of Empires and Age of Mythology games. Prior to version 1.15.2, the AoE3 POST /game/cloud/getFileURL handler in the bundled game server has no request body size limit or cap on the attacker-controlled JSON names array and allocates response storage directly from the unbounded array length. A remote unauthenticated client can use the default self-registration flow and send an oversized request that causes excessive memory allocation, crashes or hangs the server process, disconnects active players, and keeps the service unavailable until it is restarted. This issue is fixed in version 1.15.2.	7.5	More Details
CVE-2026-107838	RIOT is an open-source microcontroller operating system designed for Internet of Things devices and other embedded systems. From version 2023.07 through version 2026.07, nanocoap_fileserver callers in sys/net/application_layer/nanocoap/fileserver.c ignore a failure returned by _resp_init() when coap_build_reply() cannot fit a response header into the response buffer. A remote client can send a CoAP request with a sufficiently large extended token when nanocoap_token_ext is enabled, causing response initialization to fail while _get_file() or _get_directory() continues with stale response state. The path then reaches _calc_szx2() and its pdu->payload_len > reserve assertion, terminating the affected service or device task. No fixed release is available as of this review.	7.5	More Details
	pH7Builder (pH7 Social Dating CMS) before 18.6.0 contains a hard-coded API key vulnerability in		

CVE-2026-108905	Tool.class.php that allows unauthenticated attackers to bypass API access checks by spoofing the Host header. Attackers can send Host: localhost with private_api_key=dev772277 and the default allowed URL to retrieve member emails, IP addresses, phone numbers, and bank account fields.	7.5	More Details
CVE-2026-107826	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. From 3.0.0 until 3.8.1, readJSON in internal/bodyprocessors/json.go can stop its bounded flattening walk after reaching SecArgumentsLimit or the byte budget and then call gjson.Valid on the complete raw body. An unauthenticated attacker can submit shallow values followed by an extremely deeply nested JSON tail that was not visited by the bounded walk, causing gjson.Valid to recurse without a depth bound and terminate the hosting process with an unrecoverable fatal stack overflow. The ProcessRequest and ProcessResponse JSON paths share the affected readJSON validation flow, and the payload can remain within recommended body-size and argument-count limits. This issue is fixed in version 3.8.1.	7.5	More Details
CVE-2026-108160	AstronRPA through 1.1.6 contains a download of code without integrity check vulnerability that allows network attackers to deliver malicious updates by abusing the desktop client's auto-update mechanism. Attackers positioned between the client and server can serve a malicious update manifest and NSIS installer, which electron-updater installs without signature verification, executing code as the desktop user.	7.5	More Details
CVE-2026-75347	EIPStackGroup OpENer v2.3 and master up to commit 76b95cf contain an expired pointer dereference vulnerability in the EtherNet/IP Common Packet Format (CPF) handling logic. This allows a remote attacker to cause a denial of service.	7.5	More Details
CVE-2026-56866	When http.Transport sends an HTTP/1 CONNECT request with a non-empty Request.Body, it writes the body directly to the connection without framing after the request headers. If the server rejects the CONNECT request with a non-2xx keep-alive response, Transport returns the connection to the idle pool. Because CONNECT requests do not have a request body, the server may interpret the trailing body bytes as a subsequent pipelined HTTP/1.1 request on the connection, leaving the pooled connection desynchronized and causing the next caller that reuses it to read the response to the injected request. In reverse proxies (including httputil.ReverseProxy) that forward CONNECT requests through a shared Transport, this can lead to cross-user response poisoning.	7.5	More Details
CVE-2026-107574	Inefficient algorithmic complexity in the JSON reader of Progressive Robot hMailServer allows a remote unauthenticated attacker to make the mail services unavailable. Reading a JSON object kept the first of each duplicated member name by searching the members already read, so an object of N distinct member names cost $O(N^2)$: 1 MB took 8.9 seconds and 4 MB took 300 seconds against the affected code. A remote attacker reaches the reader without an account by mailing a crafted TLS-RPT report (up to 16 MB after decompression) to a hosted domain's published report mailbox, which is read on a delivery thread; a few such reports hold every delivery thread (ten by default), so the server delivers no mail, local or outbound, for over an hour per report. A signed-in account reaches the same 16 MB body through the webmail's own REST routes, holding the REST API's own worker threads. Where no report mailbox is configured, the unauthenticated REST sign-in routes that read a JSON body are capped at 64 KB and are not affected.	7.5	More Details
CVE-2026-108859	mcp-go through 1.2.1 contains a denial of service vulnerability in StreamableHTTPServer.ServeHTTP that allows remote unauthenticated attackers to exhaust memory by sending oversized POST bodies. Attackers can send arbitrarily large or many concurrent POST requests, read fully via io.ReadAll before validation, to degrade or OOM-kill the server process.	7.5	More Details
CVE-2026-106056	Rundeck before 6.2.0 contains an OS command injection vulnerability that allows authenticated users with job run permission to execute commands on Windows nodes by supplying crafted option values. Attackers can inject cmd.exe metacharacters such as && or into free-text options, which CLIUtils.quoteWindowsCMDArg wraps in ineffective single quotes, running commands with node executor credential privileges.	7.5	More Details
CVE-2026-19935	The Bluetooth LE host queues received L2CAP connection-oriented channel (CoC) data for deferred processing through a struct k_work embedded in the channel object (le_chan->rx_work, handler l2cap_rx_process()) whenever the channel uses a dynamic PSM (0x0080-0x00FF). Channel teardown in l2cap_chan_destroy() in subsys/bluetooth/host/l2cap.c cancels the retransmission-timeout work and drains the RX FIFO, but never cancels rx_work. Because that work item was submitted to the system workqueue while HCI receive processing runs on the dedicated Bluetooth RX workqueue (CONFIG_BT_RECV_WORKQ_BT, the default), a queued rx_work item can outlive the channel it points into. A remote, unauthenticated peer with an established CoC channel triggers this by sending a data K-frame immediately followed by an L2CAP Disconnect Request. The K-frame submits rx_work to the system workqueue; because both workqueue threads are cooperative and the Bluetooth RX workqueue runs at the higher priority (K_PRIO_COOP(CONFIG_BT_RX_PRIO) versus CONFIG_SYSTEM_WORKQUEUE_PRIORITY), the pending item cannot run before the following Disconnect Request is processed in le_disconn_req() -> l2cap_chan_del() -> l2cap_chan_destroy(). The stack then invokes the released() callback, which the API documents as meaning the stack has dropped all references and the application may free the channel memory. The application therefore frees or re-accepts into an object that the system workqueue still holds in its pending list. If the memory is freed and reallocated, the workqueue later dereferences a list node and a handler function pointer read from reused memory; if the object is re-used for a later connection, l2cap_chan_add() calls k_work_init() on a still-enqueued work item, corrupting the workqueue's pending list so that unrelated work items are	7.5	More Details

	dropped or the queue spins on a looped list. A related variant lets l2cap_rx_process() run concurrently with teardown, racing the net_buf unref of le_chan->_sdu and the clearing of chan->conn. The fix routes the channel RX work to the Bluetooth workqueue - the same context in which every teardown path runs - and adds an explicit k_work_cancel() of le_chan->rx_work in l2cap_chan_destroy(), so no reference to the channel survives the released() callback. Configurations without CONFIG_BT_L2CAP_DYNAMIC_CHANNEL, or that only use SIG-assigned PSMs (EATT 0x0027, OTS 0x0025) which take the inline receive path, are not affected.		
CVE-2026-89301	The rtMedia for WordPress, BuddyPress and bbPress plugin for WordPress is vulnerable to limited file deletion due to insufficient file path validation in the process function in all versions up to, and including, 4.7.13 This makes it possible for unauthenticated attackers to delete arbitrary safe files on the server.. The public nonce (rtmedia_upload_nonce) is emitted into frontend JavaScript on any page rendering the rtMedia gallery or upload shortcode, making it retrievable by unauthenticated visitors without any prior authentication or privileged action.	7.5	More Details
CVE-2026-94440	Parsing a multipart form can bypass memory limits and read an arbitrarily long line into memory when the remaining limit at the start of a part is less than 400 bytes.	7.5	More Details
CVE-2026-107728	Strawberry GraphQL is a library for creating GraphQL APIs. From 0.217.0 until 0.326.1, PermissionExtension.resolve() on a synchronous field resolver evaluates the result of has_permission() for truthiness. When a custom permission declares has_permission() as a normal function but returns an awaitable, supports_sync does not classify it as asynchronous, the awaitable is not awaited, and its inherently truthy object value permits the protected resolver to run even when the result would resolve to false. This affects synchronous field resolvers under both execute_sync() and execute(); permissions declared with async def has_permission() and synchronous permissions returning a boolean are not affected. This issue is fixed in version 0.326.1.	7.5	More Details
CVE-2026-108714	MCP Kotlin SDK through 0.15.0 contains an uncontrolled memory allocation vulnerability that allows remote clients to exhaust server memory because Application.mcpWebSocket installs Ktor WebSockets without a maxFrameSize limit. Attackers can send small frame headers declaring payloads near 2 GiB over one or a few connections, forcing huge heap allocations and causing denial of service.	7.5	More Details
CVE-2026-108159	AstronRPA through 1.1.6 contains a cross-site scripting vulnerability in the desktop client's smart-component chat that allows remote attackers to execute OS commands by abusing unsanitized LLM output rendered via v-html. Attackers can embed prompt-injection content in a web page so the model emits HTML event handlers invoking the unrestricted open-path IPC handler with shell metacharacters, executing commands as the desktop user.	7.5	More Details
CVE-2026-94439	When an HTTP server handler sends a 2xx response to an HTTP/1 CONNECT request and returns without hijacking the connection, the server improperly continues to read and serve requests from the connection. Since a 2xx response to an HTTP/1 CONNECT converts the connection into a tunnel, the server should not treat the connection as continuing to contain HTTP. The impact of this misbehavior is mostly limited to potential request smuggling, where an intermediate proxy considers the data on the connection to be tunneled and the server considers it to be HTTP.	7.5	More Details
CVE-2026-108739	OpenAgents Workspace backend through launcher-v1.0.17 contains an information disclosure vulnerability that allows unauthenticated attackers to list all workspaces via GET /v1/workspaces. Attackers can read the unmasked browserfabric_api_key in each workspace's settings map, along with workspace ids, slugs, creator emails and member lists.	7.5	More Details
CVE-2026-106058	GitAhead through 2.7.1 contains an OS command injection vulnerability in src/git/Filter.cpp that allows malicious repositories to execute commands by substituting crafted filenames into clean/smudge filter commands. Attackers can ship files named with \$(command) selected via .gitattributes so checkout or staging runs the command through bash -c as the victim.	7.5	More Details
CVE-2026-78669	A malicious HTTP/2 peer can cause excessive CPU consumption in the client or server by opening a large number of streams and then sending many small SETTINGS frames containing SETTINGS_INITIAL_WINDOW_SIZE values.	7.5	More Details
CVE-2026-78667	When parsing a Range header containing a large number of small ranges, FileServer(FS), ServeContent, and ServeFile(FS) can consume an excessive amount of CPU.	7.5	More Details
CVE-2026-103649	Missing network timeouts in the Linux builds of Progressive Robot hMailServer 6.3.0 through 6.3.5 allow a remote attacker to hold server threads indefinitely and so stop outbound mail delivery (denial of service). The server set its socket timeouts in the form Windows takes, which Linux refuses, and its HTTPS clients read without a deadline, so a peer that accepts a connection and then sends nothing held the waiting thread for as long as the connection stayed open. The MTA-STs policy fetch, enabled by default, is made during outbound delivery to mta-sts.<recipient domain>, so anyone who can make the server deliver mail to a domain they control - for example as the envelope sender of a message that bounces - can hold delivery threads until outbound delivery stops. The same flaw affects the DANE TLSA query, the OAuth2 token request, the ACME client, and the ManageSieve and metrics listeners, which a silent client stops from serving anyone else.	7.5	More Details

	Windows builds are not affected.		
CVE-2026-78660	Historically, we have been rather lax about malformed framing-related headers in our HTTP/2 implementation, as they cannot interfere with HTTP/2 framing. However, this makes it possible for our HTTP/2 implementation to forward responses containing such headers to an HTTP/1 client when acting as a reverse proxy. If the HTTP/1 client also does not behave strictly enough, this can result in response smuggling.	7.5	More Details
CVE-2026-104659	Missing Host header validation and missing throttling of failed administrator sign-ins in the REST API listener of Progressive Robot hMailServer 6.0.0 through 6.3.5 allow a remote attacker to brute-force the server administrator's password through the administrator's own browser by DNS rebinding. The listener, which is off by default and bound to the loopback when enabled, answered requests whatever their Host header named, and a failed sign-in with the administrator's password from the loopback was neither auto-banned nor delayed. A web page whose host name the attacker rebinds to 127.0.0.1, opened in a browser on the server, can therefore send authenticated requests to the listener, read the answers and try administrator passwords at full speed until one is accepted, giving the attacker full administrative control of the mail server.	7.5	More Details
CVE-2026-78659	When "Trailer" headers are sent by a client, the HTTP server internally uses the header values to populate the Request.Trailer map passed to the server handler. Because Request.Trailer is a map, each entry incurs memory overhead. For HTTP/2 servers, a malicious client can exploit this by sending a "Trailer" header that declares a large number of fields, causing the server to allocate a disproportionate amount of memory while bypassing Server.MaxHeaderValueCount and Server.MaxHeaderBytes limits. This exploit is not applicable for HTTP/1 servers, which do not support multiplexing a large number of requests over one TCP connection, and whose Server.MaxHeaderBytes are calculated differently.	7.5	More Details
CVE-2026-84875	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	7.5	More Details
CVE-2026-84275	IBM Guardium Data Protection 12.2 is vulnerable to path traversal in the GIM file-upload functionality. An unauthenticated attacker could exploit this vulnerability to write arbitrary files to the Collector.	7.5	More Details
CVE-2026-91136	The Divi Plus plugin for WordPress is vulnerable to Arbitrary File Read in versions up to, and including, 2.4.0 via the 'svg_image' parameter of the /wp-json/elicus/v1/dipl-modules/svg-animator REST endpoint. This is due to the endpoint's permission callback (SVGAnimatorController::index_permission) returning true unconditionally combined with insufficient validation of the 'svg_image' input — sanitize_text_field() and esc_html() do not restrict filesystem paths, the file:// stream wrapper, or arbitrary URLs — before it is passed to file_get_contents() (with a wp_remote_get() fallback) and the raw response body is returned in the JSON 'html' field. This makes it possible for unauthenticated attackers to read arbitrary files on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2026-56851	The Nickname profile can panic with an out-of-bounds slice error when transforming crafted input into a short destination buffer.	7.5	More Details
CVE-2026-93447	IBM Langflow OSS 1.0.0 through 1.12.2 could allow an attacker with access to the server secret and Redis write access to submit a malicious serialized cache value. When the value was retrieved, deserialization could have executed attacker-controlled code with the privileges of the service process.	7.5	More Details
CVE-2026-42706	Unauthenticated Broken Access Control in DK <= 3.2.1 versions.	7.5	More Details
CVE-2026-42705	Unauthenticated Broken Access Control in Grand News <= 3.4 versions.	7.5	More Details
CVE-2026-107216	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.8.1 to 2.11.0, ANCHORARRAY recursively calls the exported CalcCellValue function, creating a fresh calculation context at each cycle and bypassing in-flight and iteration controls. ANCHORARRAY calls CalcCellValue instead of cellResolver, so each recursive hop receives a new calcContext and loses cycle state. When mutually referencing dynamic-array formulas are evaluated directly or through formula-evaluating APIs, each recursion hop resets the cycle budget and prevents completion-based caches from breaking the cycle, allowing an attacker to cause a fatal Go stack overflow and abort the process. No fixed version is available as of this review.	7.5	More Details
CVE-2026-107215	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.3.1 to 2.11.0, extractPart allocates a byte slice directly from an attacker-controlled CFB directory-entry size before validating the sector chain or size domain. extractPart trusts the CFB directory entry streamSize for EncryptionInfo and EncryptedPackage allocations before validating the stream. When a crafted OLE compound file declares a negative or extremely large EncryptionInfo or EncryptedPackage stream size, the declared size reaches make with a negative length or forces a multi-gigabyte allocation, allowing an attacker to panic or exhaust process memory. No fixed version is available as of this review.	7.5	More Details

CVE-2026-107214	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.3.1 to 2.11.0, the decryption dispatch performs insufficient structural and parameter validation before standard and agile decryptors slice, index, allocate, and divide using attacker-controlled values. Decrypt passes attacker-controlled EncryptionInfo and EncryptedPackage data into standardDecrypt or agileDecrypt before validating the structures used by those routines. When a malformed OLE compound file with a version-valid EncryptionInfo stream is opened or passed to Decrypt, nine malformed-input classes reach unrecovered Go runtime panics instead of the documented error path, allowing an attacker to terminate the calling process. No fixed version is available as of this review.	7.5	More Details
CVE-2026-15822	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to improper memoization of GraphQL fragment spreads.	7.5	More Details
CVE-2026-15819	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to out-of-bounds memory access caused by a strict-weak-ordering violation in a sorting comparator.	7.5	More Details
CVE-2026-107212	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.1.0 to 2.11.0, Rows.Columns accepts a look-ahead row number above TotalRows without applying the limit enforced by Rows.Next. File.GetRows relies on Rows.Next and Rows.Columns, but Rows.Columns consumes the row r attribute without the limit check in Rows.Next. When a crafted worksheet places an oversized row number after an ordinary valid row and the application calls GetRows or iterates Rows, the iterator advances through every missing row number instead of rejecting the workbook, allowing an attacker to consume a CPU core for an attacker-controlled duration. No fixed version is available as of this review.	7.5	More Details
CVE-2026-107302	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, the decoder reads the four-byte length of a map32 value before validating that the complete five-byte header is available. A truncated map32 header therefore causes a checked out-of-bounds buffer read and throws RangeError instead of IncompleteBufferError, which can unexpectedly terminate a request, stream, or worker in applications that wait for additional bytes after IncompleteBufferError. There is no adjacent-memory disclosure because the buffer implementation checks bounds. This issue is fixed in version 6.1.0.	7.5	More Details
CVE-2026-82627	The Uncanny Automator – AI + Automation for WordPress AI Agent, AI Page Builder, Free AI Usage Included plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.6.1.1 via deserialization of untrusted input. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object when a third-party integration plugin (such as PeepSo, MailPoet, WPForms, etc) is installed and a recipe is configured that stores attacker-controlled data as trigger meta. The additional presence of a POP chain within Uncanny Automator allows attackers to delete arbitrary files on the server.	7.5	More Details
CVE-2026-65459	Unauthenticated Arbitrary Content Deletion in Forminator <= 1.57.3 versions.	7.5	More Details
CVE-2026-107805	Nginx UI is a web user interface for the Nginx web server. From 2.5.0 until 2.6.0, the node-signature authentication path performs temporary file staging of an attacker-controlled request body and synchronizes it before validating the body digest and cryptographic signature. An unauthenticated remote client that can reach the API and provide syntactically valid signature metadata can consume temporary filesystem capacity, disk input and output, and request-processing resources before rejection. The issue affects availability and does not bypass authentication or provide confidentiality or integrity impact. This issue is fixed in version 2.6.0.	7.5	More Details
CVE-2026-94664	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in add-ons.org PDF for Contact Form 7 pdf-for-contact-form-7 allows Path Traversal.This issue affects PDF for Contact Form 7: from n/a through 7.1.0.	7.5	More Details
CVE-2026-87665	A stack-based buffer overflow vulnerability exists in the Internet Key Exchange (IKEv2) protocol handler on Brocade Fabric OS versions before 10.0.1. The vulnerability occurs when processing initial IKE key exchange requests on extension switches or blades running IPsec-enabled Fibre Channel over IP (FCIP) circuits. An unauthenticated remote attacker can exploit this vulnerability by sending a single, specifically crafted UDP packet (Port 500) containing an oversized Nonce payload. Successful exploitation results in a denial of service (data-plane process crash)	7.5	More Details
CVE-2026-107589	Insufficient job validation for service accounts in Jacamar CI prior to v0.30.0 allows authenticated CI users to generate arbitrary account names.	7.5	More Details
CVE-2026-93443	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in code.	7.5	More Details
CVE-			

2026-95184	Improper certificate validation in gnutls v3.8.13 causes the application to reject legitimate certificates for valid users, leading to a Denial of Service (DoS).	7.5	More Details
CVE-2026-107232	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.12 on 3.x and 2.16.1 on 2.x, the client infers that an HTTP proxy tunnel exists from the last request method rather than the CONNECT result. After a proxy rejects CONNECT, redirect or authentication handlers can write an origin request and its Authorization credentials onto the still-plaintext proxy connection. Basic credentials can be recovered directly, while NTLM responses may be cracked or relayed. This issue is fixed in versions 3.0.12 and 2.16.1.	7.5	More Details
CVE-2026-107286	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 2.10.0 until 2.53.0, streamed requests made through ConcurrencyLimitedModel or limit_model_concurrency can retain shared concurrency slots because anyio.CapacityLimiter associates an acquired slot with the borrowing task while streaming cleanup can run in a different task. Early stream termination, cancellation, consumer exceptions, or complete stream_text() consumption with debounce_by=0.1 can therefore leave capacity occupied, eventually preventing later requests that share the long-lived limiter from proceeding and causing a denial of service. Agent-level max_concurrency and non-streaming model requests are not affected. This issue is fixed in version 2.53.0.	7.5	More Details
CVE-2026-105281	The internal data publisher on openPDC accepts network connections without authentication in its default configuration. An unauthenticated network attacker can connect to this interface and retrieve the complete device and measurement topology of the system.	7.5	More Details
CVE-2026-95116	An issue in libming through 0.4.8 allows a remote attacker to cause a denial of service via the readtag_file() in src/blocks/fromswf.c.	7.5	More Details
CVE-2026-105830	league/commonmark from 2.0.0 before 2.10.2 contains a quadratic-time denial of service vulnerability in the GitHub Flavored Markdown Table extension's TableStartParser::tryStart() block-start scan. Unauthenticated attackers can submit a large paragraph of pipe-free lines not starting with letters, forcing repeated full-buffer strtos scans that exhaust PHP worker CPU.	7.5	More Details
CVE-2026-107161	A heap-based buffer overflow flaw was found in Cyrus SASL. The add_to_challenge() function in the DIGEST-MD5 plugin computes the size of the buffer needed for a challenge/response field before DIGEST-MD5 quoting is applied, but does not recompute that size when quoting (escaping special characters) makes the value longer. The under-sized buffer is then passed to strcat(), causing a heap-based out-of-bounds write whose size depends on attacker-controlled input. A malicious or on-path DIGEST-MD5 (or HTTP Digest) server can trigger this flaw in a connecting client by supplying a crafted challenge field, such as realm or nonce, most likely resulting in a crash of the client application.	7.5	More Details
CVE-2026-107377	datamodel-code-generator generates Python data models from schema definitions. From 0.59.0 until 0.81.0, an attacker-controlled Protobuf schema can supply absolute or parent-directory paths captured by WEAK_IMPORT_PATTERN and consumed by _write_missing_weak_imports in src/datamodel_code_generator/parser/protobuf.py. Exploitation requires a victim or automated job to process the attacker-controlled schema with Protobuf input support, which requires the grpcio-tools package. The paths escape the weak_imports temporary directory before protoc runs, allowing creation of directory trees and new files or overwrite of existing writable files with a generated Protobuf syntax declaration. The effect persists when later Protobuf compilation fails. The written content is limited to a proto2 or proto3 syntax declaration, and direct arbitrary code execution has not been demonstrated. This issue is fixed in version 0.81.0.	7.5	More Details
CVE-2026-62043	Unauthenticated Sensitive Data Exposure in Contact Form 7 - Dynamic Text Extension <= 5.0.7 versions.	7.5	More Details
CVE-2026-16161	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	7.5	More Details
CVE-2026-78025	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure, Protection mechanism bypass, and Unauthorized access.	7.5	More Details
CVE-2026-107223	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.1.0 to 2.11.0, flatCols expands file-loaded column ranges without validating Min and Max against the worksheet column limit. SetColWidth reaches flatCols, which expands.xlsxCol.Min through.xlsxCol.Max without enforcing MaxColumns. When a crafted worksheet supplies an oversized col max attribute and the application invokes a column mutator, flatCols performs a deep copy and append for every attacker-selected column number, allowing an attacker to consume excessive CPU and memory or trigger OOM. No fixed version is available as of this review.	7.5	More Details

CVE-2026-16111	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow an attacker to cause a denial of service due to a type confusion flaw.	7.5	More Details
CVE-2026-107219	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.3.1 to 2.11.0, agile decryption accepts an attacker-controlled spinCount and performs that many password-key derivation iterations before verifier validation. OpenFile reaches agileDecrypt, which passes the unbounded spinCount to convertPasswdToKey before password verification. When a crafted OLE encrypted-workbook header supplies an excessive spinCount and the file is opened, the key-derivation loop performs unbounded attacker-selected work and cannot be cancelled, allowing an attacker to consume a CPU core for an attacker-controlled duration. No fixed version is available as of this review.	7.5	More Details
CVE-2026-107217	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.0.0 to 2.11.0 in github.com/xuri/excelize/v2 and from 1.1.0 to 1.4.1 in github.com/xuri/excelize, ColumnNameToNumber accumulates a bijective base-26 value in int64 without detecting overflow, allowing an invalid long column name to wrap to zero with no error. ColumnNameToNumber accepts the overflowing name VGWQHXLSDEVIKVV, after which checkSheetR0 and xlsxWorksheet.checkRow use the wrapped column value as an index. When a crafted worksheet uses an overflowing column name in a row normalized by checkSheetR0 or checkRow, the wrapped zero column becomes a negative slice index during worksheet normalization, allowing an attacker to panic and terminate the calling process. No fixed version is available as of this review.	7.5	More Details
CVE-2026-103371	Insertion of Sensitive Information into Log File in Apache Geode Web Management. This issue affects Apache Geode: from 2.0.0 before 2.0.3. Users are recommended to upgrade to version 2.0.3, which fixes the issue.	7.5	More Details
CVE-2026-96335	Missing Authorization vulnerability in WPMU DEV Forminator allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Forminator: from n/a through 1.57.2.	7.5	More Details
CVE-2026-94666	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ZealousWeb Generate PDF using Contact Form 7 generate-pdf-using-contact-form-7 allows Path Traversal.This issue affects Generate PDF using Contact Form 7: from n/a through 4.2.1.	7.5	More Details
CVE-2026-42630	Unauthenticated Sensitive Data Exposure in Web Plura Backup & Restore Manager <= 0.2.25 versions.	7.5	More Details
CVE-2026-84230	IBM Guardium Data Protection 12.2.2 could allow a remote attacker to cause a denial of service due to a race condition resulting from concurrent unsynchronized writes to a shared map.	7.5	More Details
CVE-2026-97076	Executable Regular Expression Error vulnerability in WP Media WP Rocket wp-rocket allows Code Injection.This issue affects WP Rocket: from n/a before 3.23.5.	7.5	More Details
CVE-2026-103071	Improper Control of Generation of Code ('Code Injection') vulnerability in VillaTheme Thank You Page Customizer for WooCommerce woo-thank-you-page-customizer allows Code Injection.This issue affects Thank You Page Customizer for WooCommerce: from n/a through 1.2.3.	7.5	More Details
CVE-2026-108553	OpenRefine through 3.10.1 contains a cross-site request forgery vulnerability in the get-rows command that allows remote attackers to execute Jython facet expressions. Attackers can lure a user to a malicious page issuing a cross-origin GET with a crafted engine parameter, executing operating system commands as the OpenRefine user.	7.5	More Details
CVE-2026-82212	The Nexi XPay Build WordPress plugin through 7.6.2 does not correctly validate the security token on its payment notification route, accepting the request when the target order has no stored token, which allows unauthenticated attackers to mark arbitrary orders as paid, or to mark genuinely paid orders as failed.	7.5	More Details
CVE-2026-106609	Missing Authorization vulnerability in Web Impian Bayarcash WooCommerce bayarcash-wc allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Bayarcash WooCommerce: from n/a through 4.4.2.	7.5	More Details
CVE-2026-16165	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to a null pointer dereference.	7.5	More Details
CVE-2026-28745	Usernames and passwords, including the default credentials, are stored in the configuration file using weak encryption. If the default credentials are known by a malicious user, they could obtain other credentials on the system.	7.5	More Details
CVE-	Spotweb through 1.5.8 contains an OS command injection vulnerability in the runcommand NZB handler that allows remote attackers to execute commands by publishing spots with malicious titles. Attackers can post		

2026-108546	self-signed spots over Usenet with shell metacharacters in the title, which are substituted unescaped for \$SPOTTITLE and passed to exec() when a user downloads the spot, running commands as the Spotweb PHP process.	7.5	More Details
CVE-2026-107300	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, the streaming decoder recursively invokes itself for each complete MessagePack value remaining in a chunk. A remote peer can send one chunk containing many small valid values, causing recursion proportional to the value count, exhausting the JavaScript call stack, and interrupting the process or stream. This issue is fixed in version 6.1.0.	7.5	More Details
CVE-2026-108106	Xerial snappy-java before 1.1.10.9 contains an unbounded memory allocation vulnerability that allows attackers to exhaust JVM memory by declaring a large uncompressed length in compressed input. Attackers can supply a few crafted bytes to Snappy.uncompress, uncompressString, SnappyInputStream or SnappyFramedInputStream to force allocations up to 2 GB, causing OutOfMemoryError and denial of service.	7.5	More Details
CVE-2026-103902	Improper verification of cryptographic signature vulnerability in DigiDoc libdigidocpp, DigiDoc DigiDoc4, DigiDoc DigiDoc Android, and DigiDoc DigiDoc iOS. The vulnerability allows an attacker to create forged digital signatures that are displayed a valid by affected DigiDoc software.This issue affects libdigidocpp: from 4.0.0 before 4.5.0; DigiDoc4: from 4.6.0 before 4.11.0; DigiDoc Android: from 2.7.0 before 3.1.0; DigiDoc iOS: from 2.7.0 before 3.1.0.	7.5	More Details
CVE-2026-76467	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76467 are related to issues concerning improper control of a resource through its lifetime that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-664.	7.5	More Details
CVE-2026-107383	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.5, 3.3.4, 3.4.7, and 3.5.4, the GeoJSON Polygon and MultiPolygon binary encoders size a Buffer.allocUnsafe() allocation from each ring's numeric length before confirming that the ring is an array. A malformed non-array ring can therefore reserve bytes that the writing loop skips, and the connector sends the full buffer through execute() or batch(), disclosing uninitialized Node.js heap data into a database value. The persisted data can include other users' content, session material, database credentials, or TLS key material and may propagate to backups and replicas. The text-protocol query() path is not affected. This issue is fixed in versions 3.2.5, 3.3.4, 3.4.7, and 3.5.4.	7.5	More Details
CVE-2026-108101	HortusFox (hortusfox-web) through 6.3 contains an unrestricted file upload vulnerability in PlantAttachmentModel that allows authenticated users to store files with client-supplied extensions under public/attachments/. Attackers can upload HTML or SVG files via /plants/attachments/add for stored cross-site scripting, or PHP files where .htaccess is unenforced to execute code.	7.5	More Details
CVE-2026-78019	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Inclusion of Functionality from Untrusted Control Sphere vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges, Filesystem access for attacker, and Remote execution.	7.5	More Details
CVE-2026-108161	FusionPBX through 5.6.5 contains an OS command injection vulnerability in call_recordings::download() that allows unauthenticated attackers to execute commands by placing calls with malicious caller ID values. When the record_name filename template is enabled, attackers can embed shell metacharacters like \$(...) in the Caller-ID name or number, executing commands as the web server user once a privileged user downloads multiple recordings as a ZIP.	7.5	More Details
CVE-2026-78020	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service, Information disclosure, and Remote execution.	7.5	More Details
CVE-2026-87671	An out-of-bounds memory read vulnerability exists in the web management daemon of Brocade Fabric OS versions before 10.0.1. Unauthenticated HTTP endpoints process specific URL query parameters without validating array index boundaries or performing numerical range checks. An unauthenticated remote attacker can exploit this issue by sending a single, crafted HTTP request containing extreme numerical values in the query string. This causes an invalid memory dereference, resulting in a crash of the web management process (Denial of Service) and potential temporary management-plane disruption.	7.5	More Details
CVE-2026-106029	The WeddingCity Lite WordPress plugin through 1.0.4 does not perform any authorisation or validity checks before deleting posts, pages and media attachments, allowing unauthenticated attackers to permanently delete arbitrary content site-wide.	7.5	More Details
CVE-2026-16181	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to bypass security restrictions due to improper authorization.	7.4	More Details
	Progressive Robot hMailServer 6.0.0 through 6.3.5 fails open when applying DANE (RFC 7672) to outbound		

CVE-2026-107584	SMTP delivery. The server's validating DNSSEC resolver treated a TLSA or MX lookup that did not complete (no answer, SERVFAIL, a malformed reply), an answer without the requested records and without an NSEC/NSEC3 proof of their absence, and an answer whose records carried no applicable RRSIG as if the recipient domain were unsigned, and from 6.2.19 it also delivered to mail exchangers taken from an unvalidated MX lookup that the DNSSEC-validated MX record set did not name. An attacker who can drop, forge or strip DNS answers on the path to the server's resolver, at the resolver, or between the resolver and the recipient domain's name servers, and who holds an active position on the SMTP path, can thereby disable DANE for a DNSSEC-signed recipient domain and cause messages to be delivered in cleartext or to a host of the attacker's choosing with an arbitrary certificate, where they can be read and modified.	7.4	More Details
CVE-2026-107385	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.5, 3.3.4, 3.4.7, and 3.5.4, text-protocol escaping always prefixes quotes with a backslash and does not honor the session's NO_BACKSLASH_ESCAPES mode, including in Connection.escape(). When that mode is enabled, the backslash is an ordinary character, so an attacker-controlled placeholder value can close the SQL string literal and inject arbitrary SQL with the application's database privileges. The vulnerable configuration may be enabled server-wide, through connector initialization options, or with an application-issued SET sql_mode; execute() and batch() use binary protocols and are not affected. This issue is fixed in versions 3.2.5, 3.3.4, 3.4.7, and 3.5.4.	7.4	More Details
CVE-2026-93695	In Progress ShareFile Storage Zones Controller v5.12.6 and below, FileCopyService uses a remote file identifier when constructing a local temporary file path without enforcing containment. This can cause FileCopyService to write attacker-controlled content to filesystem locations writable by the service account. This can result in remote code execution when an executable IIS-served directory is writable.	7.4	More Details
CVE-2026-107318	@fastify/reply-from is a Fastify plugin that forwards requests to an upstream HTTP or HTTPS server. In versions prior to 12.7.0, all of the built-in HTTPS transports override the secure default and set rejectUnauthorized to false, so the proxy does not verify the TLS certificate of the upstream even when the application points it at an https upstream in the default configuration. An on-path network attacker can therefore impersonate the configured HTTPS upstream, read the credentials and request bodies the proxy forwards, and return forged responses that the application trusts. The issue is fixed in @fastify/reply-from 12.7.0, and users should upgrade to 12.7.0 or later. As a workaround, pass an explicit rejectUnauthorized true on the transport, supply an already configured undici instance, or use the undici global agent.	7.4	More Details
CVE-2026-107781	Dromara Skyeye through commit 003549ae5615bd114ba5bb8ddf6a8e8ead97c321 contains a server-side request forgery and missing authorization vulnerability in the OnlyOffice save callback editUploadOfficeFileById. Unauthenticated attackers can supply arbitrary url and key parameters to make the server fetch internal URLs and overwrite any user's stored file, then read results via queryFileToShowById.	7.4	More Details
CVE-2026-107230	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. From 2.0.0 until 3.0.14, connection-pool partitioning still omits identity-defining fields for Kerberos, SPNEGO, NTLM, and authenticated proxy connections. Logins without a configured principal, proxy realms, identities sharing a user name, and SOCKS or CONNECT proxy logins can reuse a socket authenticated as a different identity. A later request is then executed under the first identity and can expose that identity's data or authority to another caller. In the affected execution path, SpnegoEngine, NTLM, Kerberos, SPNEGO, SOCKS, and CONNECT control or expose the vulnerable behavior. This issue is fixed in version 3.0.14.	7.4	More Details
CVE-2026-46572	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in ntfs_ib_cut_tail() in libntfs-3g/index.c that allows an attacker to corrupt heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered by creating a file in a specially crafted directory.	7.4	More Details
CVE-2026-107724	fast-jwt provides fast JSON Web Token (JWT) implementation. In 6.2.4, fast-jwt can classify raw serialized public JWK or JWKS JSON as an HMAC secret because src/crypto.js performDetectPublicKeyAlgorithms treats non-PEM strings as symmetric key material. If HS256 is explicitly allowed or inferred, an attacker who knows the exact serialized public-key bytes can use those bytes as an HMAC key and create a token containing arbitrary claims that createVerifier accepts. Serialization ordering or whitespace differences can prevent exploitation, and applications using supported PEM keys with an asymmetric-only algorithm allowlist are not affected. This issue is fixed in version 6.3.0.	7.4	More Details
CVE-2026-76469	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco networking engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-76469 are related to insufficient control flow management issues that are grouped under the Common Weakness Enumeration (CWE) CWE-691.	7.4	More Details
CVE-2026-104704	Progressive Robot hMailServer 6.0.0 through 6.3.5 does not enforce TLS for outbound SMTP delivery to a mail exchanger whose DNSSEC-validated TLSA records contain no DANE-EE (usage 3) record, contrary to RFC 7672 section 2.2. The server used only DANE-EE records and treated a validated TLSA record set consisting of DANE-TA (usage 2) or otherwise unusable records as if no records were published, so delivery to such a host fell back to opportunistic TLS. An attacker with an active position on the network path between the server and the recipient's mail exchanger can suppress or break the STARTTLS negotiation and cause messages to be delivered in cleartext, where they can be read and modified.	7.4	More Details

CVE-2026-16516	wolfSSH does not validate that the ECDSA curve identifier in a KEXDH_REPLY host key blob matches the algorithm negotiated during key exchange. In ParseECCPubKey() (src/internal.c), the blob's algorithm string is used to derive the curve via NameTold/wcPrimeForId without checking against the negotiated ssh->handshake->pubKeyId, and the RFC 5656 curve identifier string is discarded via GetSkip() rather than compared. An active network man-in-the-middle attacker can substitute a host key blob containing a different ECDSA curve, causing the client to import the key on the wrong curve. Because the attacker controls the private key for the substituted curve, signature verification passes. Exploitation requires an active MitM position and a lax public key check callback (e.g., TOFU, algorithm-name-only check, or fingerprint match against the parsed key).	7.4	More Details
CVE-2026-107720	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.3.1, fast-jwt createVerifier accepts an unsigned JWT when key is an empty string or null and algorithms is a non-empty allowlist. Falsy synchronous keys bypass prepareKeyOrSecret, allowedAlgorithms remains active, hasKey is false, and the empty signature avoids the verifySignature gate. An attacker can therefore submit a token containing arbitrary claims without possessing a signing key, resulting in authentication or authorization bypass. Claim validators still run, and non-empty keys, an empty key without algorithms, and the async key resolver path do not have this behavior. This issue is fixed in version 6.3.1.	7.4	More Details
CVE-2026-76779	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Restriction of Excessive Authentication Attempts vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges, Protection mechanism bypass, and Unauthorized access.	7.4	More Details
CVE-2026-14999	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to bypass authentication by forging valid JSON Web Signatures due to improper verification of cryptographic signatures.	7.4	More Details
CVE-2026-108826	A vulnerability was found in Zen Cart up to 2.2.2. This impacts the function zen_db_perform in the library includes/modules/payment/paypal.php of the component PayPal IPN Handler. Performing a manipulation of the argument txn_id results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named 557154f4fa025f51553094f47b06aa024220c48f. It is suggested to install a patch to address this issue.	7.3	More Details
CVE-2026-108806	A vulnerability has been found in krupalshah EmployeeRecruitmentSystem up to 922ff6d208278282e7c8e36d70d9ae356adec9fe. Affected by this issue is the function mysql_query of the file source/authprocessing.php of the component Forgot Password Handler. Such manipulation of the argument fpemail leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-108571	A weakness has been identified in Xinhua Rainrock RockOA up to 2.7.6. This impacts the function kqjcmdModel::returnchuli of the file webmain/task/openapi/openkqjAction.php of the component Openkqj Action. This manipulation of the argument ID 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. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-108798	A vulnerability was found in ZKTeco BioTime 9.5.6 Build 20260130.3206. This issue affects some unknown processing. The manipulation results in use of hard-coded cryptographic key . The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-91844	Unrestricted upload of file with dangerous type vulnerability in İzometri IT Services Domestic and Foreign Trade Co. Ltd. Eimzamip allows Using Malicious Files. This issue affects eimzamip: from v1.6.4 before v1.6.6.	7.3	More Details
CVE-2026-108783	A security vulnerability has been detected in PRVTPRO Amnezia-Web-Panel up to 1.6.2/1.7.2. This affects an unknown part of the file app.py of the component Backup Download. The manipulation leads to use of default credentials. The attack can 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.	7.3	More Details
CVE-2026-62038	Unauthenticated Broken Authentication in eRoom <= 1.7.1 versions.	7.3	More Details
CVE-2026-108807	A vulnerability was found in krupalshah EmployeeRecruitmentSystem up to 922ff6d208278282e7c8e36d70d9ae356adec9fe. This affects the function mysql_query of the file source/adminregister.php of the component Registration Handler. Performing a manipulation results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details

CVE-2026-108836	A vulnerability has been found in Ollama up to 0.34.1. The affected element is the function IsValid of the file types/model/name.go of the component Pull API. The manipulation leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.34.2 is sufficient to fix this issue. The identifier of the patch is dfabde4539e42ba1e1eab50a3a50b88aea7958a0. It is suggested to upgrade the affected component.	7.3	More Details
CVE-2026-108805	A flaw has been found in krupalshah EmployeeRecruitmentSystem up to 922ff6d208278282e7c8e36d70d9ae356adec9fe. Affected by this vulnerability is the function mysql_query of the file source/loginprocessing.php of the component Login Handler. This manipulation of the argument email/password causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-108819	A security flaw has been discovered in agno-agi agno up to 3.0.6/3.1.1. This vulnerability affects the function exec of the component Agent Orchestration Layer. Performing a manipulation of the argument code results in dynamically-managed code resources. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2026-62118	Unauthenticated Broken Access Control in Barcode Scanner with Inventory & Order Manager <= 1.13.1 versions.	7.3	More Details
CVE-2026-108799	A vulnerability was determined in jackq XCMS up to 3fab5342cc509945a7ce1b8ec39d19f701b89261. Impacted is the function PublicController::sendFindPwdMail of the file Admin/Home/Controller/PublicController.class.php of the component Password Recovery Mail Endpoint. This manipulation of the argument email causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-106164	In Progress® Telerik® Document Processing SpreadProcessing library, versions prior to 2026.3.1006, an infinite loop vulnerability exists when importing an XLS file with a specifically-targeted corruption, the import timeout is ignored resulting in an unresponsive CPU thread and denial of service.	7.3	More Details
CVE-2026-108548	AstronRPA through 1.1.6 contains an authentication bypass vulnerability in the OpenResty gateway's auth_handler.lua that accepts any Bearer token without validation. Unauthenticated attackers can send arbitrary Bearer values to reach /api/resource/ and /api/rpa-ai-service/ routes and spoof X-User-Id or user_id headers to act as any user.	7.3	More Details
CVE-2026-108818	A vulnerability was identified in agno-agi agno up to 2.7.3/3.0.6. This affects the function get_authentication_dependency of the file auth.py. Such manipulation of the argument security_key leads to missing authentication. The attack may be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-104677	The WP Coder WordPress plugin before 4.5.2 does not restrict access to its PHP code-execution feature to administrators, gating it on a content capability that the Editor role holds by default, which allows Editor-level users to save and execute arbitrary PHP code on the server and fully compromise the site.	7.2	More Details
CVE-2026-105872	Deserialization of Untrusted Data vulnerability in mklacroix Product Configurator for WooCommerce product-configurator-for-woocommerce allows Object Injection.This issue affects Product Configurator for WooCommerce: from n/a through 1.7.5.	7.2	More Details
CVE-2026-102173	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via registration metadata in all versions up to, and including, 6.3.1 This is due to insufficient escaping in `ExceptionalElements::image_element()`, which concatenates a user-meta value straight into an `` attribute. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute whenever a user accesses a page rendering a Kirki users collection whose image element is bound to one of the nine registration meta fields. Requires public user registration to be enabled and a published page carrying a `kirki-register` element, which prints the required element nonce into the public markup.	7.2	More Details
CVE-2026-89417	The OMGF GDPR/DSGVO Compliant, Faster Google Fonts. Easy. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 's' Search Parameter via comments-atom Feed in all versions up to, and including, 6.3.10 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. Successful exploitation requires that the front-end server serves the retained .tmp file without a Content-Type or X-Content-Type-Options header, enabling MIME-sniffing browsers such as Chromium to execute the injected script — a condition present by default on many Apache and nginx/php-fpm deployments.	7.2	More Details
CVE-	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 28.2 via deserialization of untrusted input via the 'value'		More

2026-12626	parameter. This makes it possible for authenticated attackers, with custom-level access and above, to inject a PHP Object. No known gadget chain is available.	7.2	Details
CVE-2026-107823	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the MariaDB view FRM parser did not safely encode embedded newline characters in a username. An account with CREATE USER and CREATE VIEW WITH GRANT OPTION could create a crafted username containing additional view metadata, causing the parser to interpret part of the username as security metadata and potentially escalating database privileges. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	7.2	More Details
CVE-2026-20362	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated with the affected device.	7.2	More Details
CVE-2026-96278	The WP Photo Album Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REQUEST_URI Session History in all versions up to, and including, 9.3.03.002 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. The bypass works because esc_url_raw() strips literal angle brackets but retains HTML entities, which wpEntityDecode() silently converts back to live HTML tags before jQuery('#wppa-modal-container').html() renders them.	7.2	More Details
CVE-2026-81929	The Ocean Pro Demos and Ocean eComm Treasure Box plugins for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content' parameter in all versions up to, and including, 1.5.4, and 1.8.0, respectively, due to insufficient authorization, input sanitization, and output escaping in the Popup Builder's save_popup_content AJAX action. This makes it possible for unauthenticated attackers to inject arbitrary web scripts into a published Gutenberg popup that will execute whenever a user accesses a page on which the popup is configured to display. A valid premium license, the Popup Builder module, and at least one published Gutenberg popup configured for display are required.	7.2	More Details
CVE-2026-96765	The WPO365 SEAMLESS WORDPRESS + MICROSOFT INTEGRATION (WPO365 LOGIN) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id_token' parameter in all versions up to, and including, 44.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload is stored in the wpo365_errors transient for up to three days by submitting a crafted unauthenticated request with a forged id_token whose base64url-decoded unique_name or iss claim contains malicious HTML, requiring no prior authentication or user interaction beyond an administrator later visiting the WPO365 wizard page.	7.2	More Details
CVE-2026-107657	The HivePress – Business Directory, Listings & Classified Ads Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<custom user attribute field name, e.g. profile_test>' parameter in all versions up to, and including, 1.7.31 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. This requires an administrator to have configured a text-type custom user attribute whose display format places %value% inside an HTML attribute context (e.g., the documented pattern Custom link), and for front-end user profiles to be enabled — both of which reflect the plugin's standard, documented configuration.	7.2	More Details
CVE-2026-107207	LMCache through 0.5.5 contains a server-side request forgery vulnerability in its frontend monitoring service that allows unauthenticated attackers to bypass the proxy allowlist by registering arbitrary hosts. Attackers can add entries via POST /api/proxies and then use /proxy or /proxy2 to reach internal hosts, read responses, and tamper with nodes or stop the heartbeat.	7.2	More Details
CVE-2026-104680	The Envira Gallery WordPress plugin before 1.16.2 does not verify that a user holds the capability WordPress reserves for installing Envira Gallery WordPress plugin before 1.16.2 code before processing its setup-wizard Envira Gallery WordPress plugin before 1.16.2-installation request, and does not restrict the installation to its own curated list, allowing a Multisite subsite Administrator to install an arbitrary WordPress.org-published Envira Gallery WordPress plugin before 1.16.2 into the network-shared Envira Gallery WordPress plugin before 1.16.2 directory, a privilege Multisite reserves for the network Super Admin.	7.2	More Details
CVE-2026-94676	Deserialization of Untrusted Data vulnerability in Tainacan Community Tainacan tainacan allows Object Injection.This issue affects Tainacan: from n/a through 1.3.0.	7.2	More Details
CVE-2026-106608	Incorrect Privilege Assignment vulnerability in Automattic WooCommerce woocommerce allows Privilege Escalation.This issue affects WooCommerce: from 9.8.0 through 11.1.2.	7.2	More Details
CVE-	The Molongui Authorship – Author Boxes, Guest Authors & Co-Authors for WordPress plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'comment (href attribute inside comment content)' parameter in all versions up to, and including, 5.2.12 due to insufficient input sanitization and		

2026-101920	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. This is exploitable in the free build because the plugin's author-filter rewriter never appends the ?m_bm=true marker to its own anchors (Plugin::has_pro() returns false), meaning every href the byline script selects and rewrites is fully attacker-controlled.	7.2	More Details
CVE-2026-62044	Deserialization of Untrusted Data vulnerability in bPlugins Super Video Player super-video-player allows Object Injection.This issue affects Super Video Player: from n/a through 1.8.13.	7.2	More Details
CVE-2026-27350	Server-Side Request Forgery (SSRF) vulnerability in Builderius.io Builderius allows Server Side Request Forgery. This issue affects Builderius: from 1.4 through 1.4-beta.	7.2	More Details
CVE-2026-62130	Shop manager PHP Object Injection in WooCommerce Multilingual & Multicurrency <= 5.5.8 versions.	7.2	More Details
CVE-2026-87679	When Brocade Fabric OS versions before 10.0.1 processes trunk configuration operations, the application parses user-supplied list strings into dynamically allocated heap arrays without enforcing boundary checks on the maximum allowable number of elements. An authenticated administrator can exploit this vulnerability via crafted REST API requests containing an excessive number of list delimiters, causing heap corruption that can result in service crash or arbitrary code execution.	7.2	More Details
CVE-2026-89322	Vault and Vault Enterprise did not consistently evaluate ACL policies against the canonical form of resource and policy names. This may allow an authenticated user with delegated permissions to bypass an explicit deny restriction and access a protected resource or assign a denied policy, potentially leading to privilege escalation. This vulnerability (CVE-2026-89322) is fixed in Vault Community Edition 2.1.2, and Vault Enterprise 2.1.2, 1.21.12, 1.20.17, and 1.19.23.	7.2	More Details
CVE-2026-94568	Deserialization of Untrusted Data vulnerability in WP Hosting AS Pay with Vipps for WooCommerce woo-vipps allows Object Injection.This issue affects Pay with Vipps for WooCommerce: from n/a through 6.2.0.	7.2	More Details
CVE-2026-62030	Unauthenticated Server Side Request Forgery (SSRF) in StreamCast <= 2.4.5 versions.	7.2	More Details
CVE-2026-104021	The Fastcache by Host.it plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.7.4 via the `fastcache_settings[cache_cookie_exclude][]` parameter. This is due to the plugin registering the `cache_cookie_exclude` setting via `register_setting()` without a `sanitize_callback`, while `buildSiteHtaccessRules()` applies only `trim()` to each cookie value before interpolating it directly into an Apache `RewriteCond` line — a normalization that strips surrounding whitespace but leaves embedded newlines intact, allowing an attacker to break out of the capture group and append arbitrary directives. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary Apache directives into the site's `.htaccess` file via `file_put_contents()`, enabling server-level configuration changes such as setting `php_value auto_prepend_file` to execute attacker-controlled PHP code on every request.	7.2	More Details
CVE-2026-106606	Deserialization of Untrusted Data vulnerability in YITH YITH WooCommerce Affiliates yith-woocommerce-affiliates allows Object Injection.This issue affects YITH WooCommerce Affiliates: from n/a through 3.31.0.	7.2	More Details
CVE-2026-100178	The WPAdverts - Classifieds Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'adverts_location' parameter in all versions up to, and including, 2.3.4 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-2026-96682	The Presto Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via <presto-player> Tag in all versions up to, and including, 4.5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires an initial comment approval, though WordPress default settings will auto-approve all subsequent comments from the same author, allowing a patient unauthenticated attacker to land the payload without further admin intervention.	7.2	More Details
CVE-2026-104082	SmarterMail before build 9777 contains a remote code execution vulnerability that allows an attacker holding a SysAdmin-scoped access token to bypass the Volume Mount script-directory containment control by provisioning a new mail domain with an arbitrary FileStore root path inside the trusted Scripts directory via the domain-put endpoint. Attackers can disclose the Scripts path through the AddOrUpdateMount endpoint, clear the upload extension blacklist via the global-mail endpoint, then upload a malicious script through the ordinary mail file-storage upload API so that saving a CommandMount triggers RunScript before validation, resulting in a reverse shell executing as the SmarterMail service account with SYSTEM-level privileges.	7.2	More Details

CVE-2026-102257	A Zip Slip vulnerability in the in the SMA1000 Appliance Management Console (AMC) interface allows an attacker to extract files outside the intended destination directory using a specially crafted archive, resulting in remote code execution.	7.2	More Details
CVE-2026-104752	The Rank Math SEO WordPress plugin before 1.0.280 does not correctly validate the type of a file uploaded through its settings import feature, allowing users with administrator-level access to upload a PHP file and achieve remote code execution.	7.2	More Details
CVE-2026-14335	The Easy Digital Downloads – eCommerce Payments and Subscriptions made easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via PayPal IPN Parameters in all versions up to, and including, 3.6.9 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-2026-84278	IBM Guardium Data Protection 12.2 is affected by a command injection vulnerability in the SUID-root ssh_config_wrapper component. An authenticated high-privileged user can inject arbitrary commands through attacker-controlled arguments, resulting in command execution with root privileges.	7.2	More Details
CVE-2026-85126	The Crowdfundly WordPress plugin through 2.2.2 does not have capability checks on some of its AJAX actions, allowing users holding one of its own low privileged roles to grant themselves the administrator role or arbitrary capabilities, leading to a full site takeover.	7.2	More Details
CVE-2026-93775	The Podlove Podcast Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Auphonic Webhook in all versions up to, and including, 4.5.6 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. The injection is triggered by submitting a request to the Auphonic webhook endpoint with any POST body where the status_string field is not the literal string 'Done', causing the full raw POST superglobal to be stored in the plugin log before any authentication key validation is performed.	7.2	More Details
CVE-2026-100147	The FunnelKit – Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shipping_first_name' parameter in all versions up to, and including, 3.16.0.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-96667	The Real Estate Manager – Property Listing and Agent Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'first_name' parameter in all versions up to, and including, 7.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The reCAPTCHA check is trivially bypassed by omitting the g-recaptcha-response parameter entirely, since validation only runs when that parameter is present.	7.2	More Details
CVE-2026-100161	The Photo Reviews for WooCommerce plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'wcp_r_image_upload_id' parameter in all versions up to, and including, 1.2.30 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. The publicly-emitted `wcp_r_image_upload` nonce printed on every product review form is the only gate, and no capability, authentication, or attachment ownership check is performed, allowing the payload to be stored in comment meta — which is not subject to `wp_kses` — by any unauthenticated visitor; the XSS fires once the review is visible on the frontend.	7.2	More Details
CVE-2026-100196	The LazyLoad Plugin – Lazy Load Images, Videos, and Iframes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment_content (rendered inline into the page HTML)' parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. WordPress core's wp_kses_data allow-list does not strip the crafted payload on save because it uses only permitted tags and attributes; the event handler is concealed inside a broken attribute region and is only promoted to a real DOM attribute by the plugin's render-time str_replace transformation. Additionally, a site administrator must approve the crafted comment before the payload is served to other visitors.	7.2	More Details
CVE-2026-107742	The 10Web Booster – Website speed optimization, Cache & Page Speed optimizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' parameter in all versions up to, and including, 2.34.8 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. This is exploitable because a comment author Name value containing ' src=' and an event-handler payload contains no HTML tags or quote characters, allowing it to survive WordPress core's sanitize_text_field and land verbatim inside the alt attribute, where the plugin's own str_replace subsequently injects the single quote that breaks out of the attribute context.	7.2	More Details
CVE-	The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'attachments[name]' Parameter in all versions up to, and including, 1.8.15 due to insufficient input		More

2026-95684	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	Details
CVE-2026-96558	The Quiz and Survey Master (QSM) – Quiz Maker & Survey Maker plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'qsm_hidden_questions' parameter in all versions up to, and including, 11.2.6 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. This requires the attacker to force the mlw_results INSERT to fail by submitting an over-length or duplicate qsm_unique_key value, which triggers the audit trail code branch that writes the unescaped payload to wp_mlw_qm_audit_trail.form_data.	7.2	More Details
CVE-2026-96572	The WP Meteor Website Speed Optimization Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Author Name in all versions up to, and including, 3.4.18 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. The payload is delivered via the comment author name field, which must clear WordPress's comment moderation workflow before being displayed, though this represents a display prerequisite rather than any sanitization control.	7.2	More Details
CVE-2026-96840	The Post Grid Gutenberg Blocks – PostX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via display_name User Field in all versions up to, and including, 5.1.0 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. WordPress core's pre_user_display_name filter encodes &, <, and > but leaves double-quotes intact (ENT_NOQUOTES), allowing a Subscriber-level user to store a double-quote in their display_name via /wp-admin/profile.php that subsequently breaks out of the alt="" attribute at Archive_Title.php:144.	7.2	More Details
CVE-2026-94058	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bracketweb Treck treck allows Reflected XSS.This issue affects Treck: from n/a through 1.0.0.	7.1	More Details
CVE-2026-94059	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bracketweb Ogency ogency allows Reflected XSS.This issue affects Ogency: from n/a through 1.0.0.	7.1	More Details
CVE-2026-94060	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bracketweb Voldor voldor allows Reflected XSS.This issue affects Voldor: from n/a through 1.0.0.	7.1	More Details
CVE-2026-94061	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Designthemes Whistle - Sports Club whistle-sports-club allows Reflected XSS.This issue affects Whistle - Sports Club: from n/a through 4.2.	7.1	More Details
CVE-2026-94415	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Muffingroup Betheme betheme allows Reflected XSS.This issue affects Betheme: from n/a through 28.5.8.	7.1	More Details
CVE-2026-96607	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms nex-forms-express-wp-form-builder allows Reflected XSS.This issue affects NEX-Forms: from n/a through 9.3.1.	7.1	More Details
CVE-2026-105883	Missing Authorization vulnerability in ThemeHunk Th Shop Mania th-shop-mania allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Th Shop Mania: from n/a through 1.9.1.	7.1	More Details
CVE-2026-94668	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dimitri Grassi Salon booking system salon-booking-system allows Reflected XSS.This issue affects Salon booking system: from n/a through 10.31.5.	7.1	More Details
CVE-2026-94167	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Extend Themes Kubio AI Page Builder kubio allows Reflected XSS.This issue affects Kubio AI Page Builder: from n/a through 2.9.3.	7.1	More Details
CVE-2026-94166	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UpSolution UpSolution Core us-core allows Reflected XSS.This issue affects UpSolution Core: from n/a through 8.44.	7.1	More Details
CVE-2026-94161	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Restaurant grandrestaurant allows Reflected XSS.This issue affects Grand Restaurant: from n/a before 7.0.11.	7.1	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KlbTheme Total Donations totaldonations allows Stored XSS.This issue affects Total Donations: from n/a	7.1	More Details

94159	through 2.0.5.		
CVE-2026-94158	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bkninja Gloria Admin Panel gloria-admin-panel allows Reflected XSS.This issue affects Gloria Admin Panel: from n/a through 1.3.	7.1	More Details
CVE-2026-107362	Malcolm file-upload component ships the upstream FilePond PHP server (pqina/filepond-server-php) largely unmodified: Dockerfile copies all upstream *.php files and Malcolm only overwrites config.php and submit.php. Upstream index.php exposes a fetch API route that instructs the server to download an arbitrary URL with curl (including FOLLOWLOCATION) and, for HEAD requests, stores the fetched response body in the upload container's transfer directory and returns the transfer ID to the caller, enabling full readback of the fetched content.	7.1	More Details
CVE-2026-107337	The Malcolm kiosk Flask application exposes a POST /script_call/<script> endpoint with zero authentication and wildcard CORS (CORS(app)). An attacker can force the operator's browser to execute arbitrary management commands via CSRF, including control.py --wipe which permanently deletes all captured network traffic and forensic logs, or control.py --stop which blinds the security monitoring.	7.1	More Details
CVE-2026-94632	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stiofan BlockStrap Page Builder - Bootstrap Blocks blockstrap-page-builder-blocks allows Reflected XSS.This issue affects BlockStrap Page Builder - Bootstrap Blocks: from n/a through 0.1.58.	7.1	More Details
CVE-2026-94641	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stiofan UsersWP userswp allows Reflected XSS.This issue affects UsersWP: from n/a through 1.2.73.	7.1	More Details
CVE-2026-94661	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetBlog jet-blog allows Reflected XSS.This issue affects JetBlog: from n/a through 2.4.10.	7.1	More Details
CVE-2026-78023	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Authorization Bypass Through User-Controlled Key vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.1	More Details
CVE-2026-50054	An authorization flaw in Zimbra Collaboration Suite's GrantRightsRequest allows an attacker with access to an authenticated account to grant another local account the loginAs right, creating persistent mailbox access and mail-sending authority that survives password changes and session expiry.	7.1	More Details
CVE-2026-105870	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Delight Star Inc. WP Associate Post R2 wp-associate-post-r2 allows Reflected XSS.This issue affects WP Associate Post R2: from n/a through 5.0.1.	7.1	More Details
CVE-2026-95591	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows Reflected XSS.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.14.	7.1	More Details
CVE-2026-95596	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mamunur Rashid ShopBuilder - Elementor WooCommerce Builder Addons shopbuilder allows Reflected XSS.This issue affects ShopBuilder - Elementor WooCommerce Builder Addons: from n/a through 3.4.1.	7.1	More Details
CVE-2026-95598	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codepeople Search in Place search-in-place allows Reflected XSS.This issue affects Search in Place: from n/a through 1.5.5.	7.1	More Details
CVE-2026-106145	In Progress® Telerik® Report Server prior to version 12.2.26.1007, incorrect privilege assignment in the service-agent SignalR hub allows an authenticated user, including a low-privilege or guest account with a valid bearer token, to register as a trusted service agent. On the next server settings-synchronization event, the rogue agent receives storage settings and encryption private keys. This privilege escalation enables disclosure of protected secrets, including stored data-source credentials and connection strings, and allows agent impersonation and interference with task dispatch.	7.1	More Details
CVE-2026-95608	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginUs.Net HUSKY woocommerce-products-filter allows Reflected XSS.This issue affects HUSKY: from n/a through 1.4.3.2.	7.1	More Details
CVE-2026-95609	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant media-library-assistant allows Stored XSS.This issue affects Media Library Assistant: from n/a through 3.41.	7.1	More Details
CVE-2026-96332	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yalla ya! Simple Payment simple-payment allows Reflected XSS.This issue affects Simple Payment: from n/a through 2.5.4.	7.1	More Details
CVE-			

2026-40804	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kodezen LLC aBlocks ablocks allows Reflected XSS.This issue affects aBlocks: from n/a through 2.16.0.	7.1	More Details
CVE-2026-96553	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Damian Góra FiboSearch ajax-search-for-woocommerce allows Reflected XSS.This issue affects FiboSearch: from n/a through 1.34.1.	7.1	More Details
CVE-2026-96761	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Welcart Welcart e-Commerce usc-e-shop allows Reflected XSS.This issue affects Welcart e-Commerce: from n/a through 2.12.3.	7.1	More Details
CVE-2026-105318	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Datasolution AcyMailing SMTP Newsletter acymailing allows Reflected XSS.This issue affects AcyMailing SMTP Newsletter: from n/a through 11.1.0.	7.1	More Details
CVE-2026-94170	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Heateor Support Sassy Social Share sassy-social-share allows Reflected XSS.This issue affects Sassy Social Share: from n/a through 3.3.79.	7.1	More Details
CVE-2026-97263	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Greg Winiarski WPAdverts wpadverts allows Stored XSS.This issue affects WPAdverts: from n/a through 2.3.4.	7.1	More Details
CVE-2026-62116	Unauthenticated Cross Site Scripting (XSS) in Barcode Scanner with Inventory & Order Manager <= 1.13.1 versions.	7.1	More Details
CVE-2026-42709	Unauthenticated Cross Site Scripting (XSS) in Food Menu – Restaurant Menu & Online Ordering for WooCommerce <= 6.0.5 versions.	7.1	More Details
CVE-2026-43976	wger is a free, open-source workout and fitness manager. Prior to version 2.6, five gym management views in wger apply a flawed gym-scope guard (<code>` gym_a != gym_b`</code>) that silently passes when both operands are <code>`None`</code> . A trainer with <code>` gym.gym_trainer`</code> and <code>` gym.add_adminusernote`</code> permissions and no gym assignment (<code>` gym=None`</code>) can read private admin notes, uploaded documents, gym contracts, user configuration, and user permission data for any other unaffiliated user on the instance. The subsequent <code>querysets</code> filter only on the attacker-supplied <code>` member_id`</code> with no secondary gym-scoped validation, so all records are disclosed. Version 2.6 fixes the issue.	7.1	More Details
CVE-2026-46434	wger is a free, open-source workout and fitness manager. Prior to version 2.6, a user with only the <code>` gym_trainer`</code> permission can deactivate any account in the same gym, including <code>` gym_manager`</code> and <code>` general_gym_manager`</code> accounts. The <code>` UserDeactivateView`</code> grants access to anyone holding any one of <code>` gym.manage_gym`</code> , <code>` gym.manage_gyms`</code> , or <code>` gym.gym_trainer`</code> (OR logic via <code>` WgerMultiplePermissionRequiredMixin`</code>), and performs no privilege-hierarchy check to prevent a lower-privileged role from disabling a higher-privileged one. Version 2.6 fixes the issue.	7.1	More Details
CVE-2026-91829	The Subscribe to Comments WordPress plugin before 2.3.3 does not properly validate a parameter before reflecting it into a link target, allowing unauthenticated attackers to perform Reflected Cross-Site Scripting via a crafted URL against anyone who clicks it, including administrators.	7.1	More Details
CVE-2026-93949	Authentication Bypass Using an Alternate Path or Channel vulnerability in Omegathemes Grocery Shopping Store grocery-shopping-store allows Password Recovery Exploitation.This issue affects Grocery Shopping Store: from n/a through 1.3.3.	7.1	More Details
CVE-2026-93951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bracketweb Zeinet zeinet allows Reflected XSS.This issue affects Zeinet: from n/a through 1.0.0.	7.1	More Details
CVE-2026-106560	Backstage is an open framework for building developer portals. Prior to 0.3.25, the <code>@backstage/plugin-scaffolder-backend-module-confluence-to-markdown</code> package is affected by improper repository path validation in a scaffolder backend module. An authenticated user who can execute an affected template and control its repository file location may cause generated content to be written outside the task workspace, within locations writable by the Backstage backend process. This issue is fixed in version 0.3.25.	7.1	More Details
CVE-2026-102388	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Forminator forminator allows Stored XSS.This issue affects Forminator: from n/a through 1.57.3.	7.1	More Details
CVE-2026-62034	Unauthenticated Cross Site Scripting (XSS) in Before After Image Comparison – Image comparison for WP <= 1.1.21 versions.	7.1	More Details
CVE-			

2026-62027	Unauthenticated Cross Site Scripting (XSS) in Team Section Block <= 2.0.4 versions.	7.1	More Details
CVE-2026-57742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeREX Group Kids Planet allows Reflected XSS. This issue affects Kids Planet: from n/a through 2.2.14.2.	7.1	More Details
CVE-2026-42715	Unauthenticated Cross Site Scripting (XSS) in Photo Gallery by 10Web <= 1.8.47 versions.	7.1	More Details
CVE-2026-97264	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Greg Winiarski WPAdverts wpadverts allows Reflected XSS.This issue affects WPAdverts: from n/a through 2.3.4.	7.1	More Details
CVE-2026-42711	Unauthenticated Cross Site Scripting (XSS) in Slider by 10Web <= 1.2.63 versions.	7.1	More Details
CVE-2026-107270	Gophish through 0.12.1 contains an insecure direct object reference vulnerability that allows authenticated users to take over other users' groups, templates, landing pages and sending profiles. Attackers can supply another user's sequential id in POST requests to /api/groups/, /api/templates/, /api/pages/ or /api/sntp/ to overwrite and reassign objects, locking out owners and exposing victims' recipient lists.	7.1	More Details
CVE-2026-42617	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in ntfs_ir_to_ib() in index.c that allows an attacker to corrupt heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered by extending a directory, e.g., by creating a file.	7.1	More Details
CVE-2026-108695	MultiVendorX WordPress plugin through 5.0.19 contains an incorrect authorization vulnerability that allows vendor accounts to modify marketplace-wide settings via the settings REST endpoint. Attackers with the store_owner role can send POST requests to /wp-json/multivendorx/v1/settings, gated only by edit_stores, to overwrite commission, payout, and onboarding settings.	7.1	More Details
CVE-2026-94160	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themeStek ThemeStek Extras for LabtechCO Theme themestek-labtechco-extras allows Reflected XSS.This issue affects ThemeStek Extras for LabtechCO Theme: from n/a through 8.4.	7.1	More Details
CVE-2026-57806	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in drfuri Martfury - WooCommerce Marketplace WordPress Theme martfury allows Reflected XSS.This issue affects Martfury - WooCommerce Marketplace WordPress Theme: from n/a through 3.3.9.	7.1	More Details
CVE-2026-42702	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS tutor allows Reflected XSS.This issue affects Tutor LMS: from n/a through 4.1.0.	7.1	More Details
CVE-2026-39799	Unauthenticated Cross Site Scripting (XSS) in WP File Download <= 6.3.6 versions.	7.1	More Details
CVE-2026-108623	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysLogController deleteBatch handler that allows any authenticated user to delete system audit log entries. Low-privileged attackers can send a DELETE request with ids set to allclear to wipe the entire sys_log table, erasing all users' audit trails.	7.1	More Details
CVE-2026-39800	Unauthenticated Cross Site Scripting (XSS) in Additional Order Filters for WooCommerce <= 1.24 versions.	7.1	More Details
CVE-2026-40803	Unauthenticated Cross Site Scripting (XSS) in Jotform – AI Chatbot <= 3.8.2 versions.	7.1	More Details
CVE-2026-78534	Unauthenticated Cross Site Scripting (XSS) in Educavo <= 3.4.2 versions.	7.1	More Details
CVE-2026-78532	Unauthenticated Cross Site Scripting (XSS) in LMS <= 8.3 versions.	7.1	More Details
CVE-2026-42631	Unauthenticated Cross Site Scripting (XSS) in Qode Music <= 2.1.8.2 versions.	7.1	More Details

CVE-2026-42632	Unauthenticated Cross Site Scripting (XSS) in Qode Real Estate <= 1.1.7.3 versions.	7.1	More Details
CVE-2026-42693	Unauthenticated Cross Site Scripting (XSS) in Jannah <= 7.6.5 versions.	7.1	More Details
CVE-2026-42699	Unauthenticated Cross Site Scripting (XSS) in FV Player 8 <= 8.1.8 versions.	7.1	More Details
CVE-2026-42618	In NTFS-3G before 2026.7.7, a heap buffer overflow exists in ntfs_decompress() in compress.c that allows an attacker to corrupt one byte of heap memory in the SUID-root ntfs-3g binary by crafting a malicious NTFS image. The overflow is triggered by reading the special crafted file.	7.1	More Details
CVE-2026-62037	Unauthenticated Cross Site Scripting (XSS) in Document Embedder <= 2.4.0 versions.	7.1	More Details
CVE-2026-94670	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Everest Forms allows Reflected XSS. This issue affects Everest Forms: from n/a through 3.6.1.	7.1	More Details
CVE-2026-94063	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeREX Education Center education allows Reflected XSS.This issue affects Education Center: from n/a through 3.6.12.	7.1	More Details
CVE-2026-94066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SpabRice Pond pond allows Reflected XSS.This issue affects Pond: from n/a through 2.6.1.	7.1	More Details
CVE-2026-62100	Unauthenticated Cross Site Scripting (XSS) in KuteShop <= 4.2.9 versions.	7.1	More Details
CVE-2026-108108	PHPNuxBill through 2025.3.20 contains an authentication bypass vulnerability in RADIUS CHAP verification because Password::chap_verify() returns true when the supplied response does not match. Attackers who know a valid customer or PPPoE username can log in through MikroTik hotspot or PPPoE CHAP with any incorrect password to obtain network access and consume that customer's plan.	7.1	More Details
CVE-2026-29797	No authentication is required when updating firmware or bootloader, making it easy for malicious files to be pushed to the device. Additionally, anyone with the same software can scan a network for N-Tron devices and push/pull firmware without authenticating by using SNMP/TFTP.	7.1	More Details
CVE-2026-109164	TDuck survey form through 6.0 contains an insecure direct object reference vulnerability that allows authenticated users to delete other users' form submissions by supplying arbitrary submission ids. Attackers can place their own formKey in the path and iterate sequential submission ids in the request body to permanently delete submissions platform-wide.	7.1	More Details
CVE-2026-107611	An out-of-bounds read vulnerability in the ZRLE decoder of GlavSoft TightVNC Viewer for Windows before 2.8.88 allows a malicious or compromised VNC server to read heap memory beyond the palette allocation and crash the viewer by sending ZRLE-encoded tiles whose palette indices exceed the declared palette size. readPaletteRleTile() and readPackedPaletteTile() use the attacker-supplied index to look up colours without validating it against the palette size; out-of-bounds heap data is copied into the framebuffer (garbled display) or the read faults, terminating the viewer.	7.1	More Details
CVE-2026-66479	Cross-Site Request Forgery (CSRF) vulnerability in Liquid Web / StellarWP WPComplete wpcomplete allows Stored XSS.This issue affects WPComplete: from n/a through 2.9.5.6.	7.1	More Details
CVE-2026-105412	An SQL Injection vulnerability affecting Tuleap Enterprise Edition 17.5 could allow an attacker to have read access the Tuleap database.	7.1	More Details
CVE-2026-62026	Cross-Site Request Forgery (CSRF) vulnerability in MIGHTYminnow Dashboard Notes dashboard-notes allows Cross Site Request Forgery.This issue affects Dashboard Notes: from n/a through 1.0.3.	7.1	More Details
CVE-2026-106611	Cross-Site Request Forgery (CSRF) vulnerability in WPMU DEV Forminator forminator allows Cross Site Request Forgery.This issue affects Forminator: from n/a through 1.57.3.	7.1	More Details
	LobsterAI 2026.5.27 through 2026.9.23 contains an external control of file path vulnerability in the		

CVE-2026-108156	skills:delete IPC handler that trusts the openclawSourceDir value from a skill's _meta.json during uninstall. Attackers who convince a user to install a crafted skill can make uninstallation recursively delete arbitrary user-writable directories, such as the home directory, since the security scanner never inspects _meta.json.	7.1	More Details
CVE-2026-62064	Unauthenticated Cross Site Scripting (XSS) in Ambed <= 1.0.0 versions.	7.1	More Details
CVE-2026-95595	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fontspugin Disable and Remove Google Fonts GDPR & DSGVO friendly disable-remove-google-fonts allows Reflected XSS. This issue affects Disable and Remove Google Fonts GDPR & DSGVO friendly: from n/a through 2.0.2.	7.1	More Details
CVE-2026-62095	Unauthenticated Cross Site Scripting (XSS) in Biolife <= 3.2.3 versions.	7.1	More Details
CVE-2026-105316	The Magee Shortcodes WordPress plugin through 2.1.1 does not sanitise and escape user input in some of its AJAX actions, which are available to unauthenticated users, before reflecting it back in the response, leading to Reflected Cross-Site Scripting.	7.1	More Details
CVE-2026-87971	The If-So Dynamic Content WordPress plugin before 1.10.2 does not validate the URL scheme of a request-supplied value before reflecting it into a link on an admin page, allowing attackers to execute arbitrary JavaScript in the browser of a logged-in user who opens a crafted link.	7.1	More Details
CVE-2026-62093	Unauthenticated Cross Site Scripting (XSS) in TechOne <= 3.0.3 versions.	7.1	More Details
CVE-2026-108985	ZDR decoding in libnfs through 6.0.2 before 7613236 has an out-of-bounds write related to lib/libnfs-zdr.c with libnfs_zdr_bytes(), libnfs_zdr_string(), and libnfs_zdr_array(). The caller-supplied maxsize value is not honored.	7.1	More Details
CVE-2026-19577	net_route_ipv6_packet() in subsys/net/ip/route_ipv6.c resolved the nexthop's link-layer address with net_nbr_get_lladdr(nbr->idx) without first checking whether the neighbor cache entry actually had a linked link-layer address. An unresolved neighbor carries idx == NET_NBR_LLADDR_UNKNOWN (0xff), and net_nbr_get_lladdr() in subsys/net/ip/nbr.c performs no runtime bounds check beyond a NET_ASSERT, returning &net_neighbor_lladdr[255] — roughly 2.5 KB past the end of an array whose default size is CONFIG_NET_IPV6_MAX_NEIGHBORS (8). Because the returned pointer is never NULL, the following lladdr == NULL guard does not catch it. The function is reached from ipv6_route_packet() in subsys/net/ip/ipv6.c for every received unicast IPv6 packet whose destination is not a local address on the receiving interface; CONFIG_NET_IPV6_ROUTE is enabled by default whenever the IPv6 neighbor cache is, so no router or forwarding configuration is needed. net_route_ipv6_get_info() returns the packet's destination itself as the nexthop when a neighbor cache entry for it exists, and the cache lookup does not skip INCOMPLETE entries. An unauthenticated attacker on the same link can therefore force the unresolved state — for example by eliciting traffic to a spoofed, non-existent neighbor address so that net_ipv6_send_ns() creates an INCOMPLETE entry, or by sending a Router Advertisement with no source link-layer address option, which creates a persistently unresolved router neighbor — and then send a packet addressed to that neighbor. The result is an out-of-bounds read at a fixed index past the neighbor link-layer address array. On builds with CONFIG_ASSERT enabled the assertion fires and the device panics, giving a repeatable remote denial of service. With assertions disabled, the stale out-of-bounds struct net_linkaddr drives a memcmp() over an attacker-uninfluenced length and, when its len byte passes the NET_LINK_ADDR_MAX_LENGTH check, up to 8 bytes of unrelated static RAM are copied into the outgoing frame's destination link-layer address and transmitted on the link, disclosing them to any listener. There is no out-of-bounds write and the offset is not attacker-controlled, which bounds the impact.	7.1	More Details
CVE-2026-62091	Unauthenticated Cross Site Scripting (XSS) in Armania <= 1.4.8 versions.	7.1	More Details
CVE-2026-108913	omarchy-theme-set in Omarchy 4 before 4.0.1 allows code execution via a third-party theme because the files placed into ~/.local/state/omarchy/current/theme may include executable content from an untrusted Git repository.	7.1	More Details
CVE-2026-62082	Unauthenticated Cross Site Scripting (XSS) in Pin WP <= 7.0 versions.	7.1	More Details
CVE-	An authorization vulnerability in Apache DolphinScheduler allows authenticated non-admin users to retrieve Kubernetes configuration data intended for administrator-managed cluster configuration. The exposed kubeconfig data contains credentials that may allow users to authenticate directly to the Kubernetes API		

2026-71895	outside DolphinScheduler. The impact depends on the permissions granted to the disclosed credentials. If the kubeconfig provides cluster-admin or broadly privileged service-account access, an attacker may read Kubernetes Secrets, create pods, and establish persistent access to the cluster. This issue affects Apache DolphinScheduler: from 3.2.0 before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	7.1	More Details
CVE-2026-94662	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Stored XSS. This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.19.	7.1	More Details
CVE-2026-71183	An authorization vulnerability in Apache DolphinScheduler allows authenticated users to obtain information about data sources they are not authorized to access through the /unauth-datasource and /authed-datasource endpoints. These endpoints fail to enforce the required data source access controls and return sensitive connection information, including data source passwords. As a result, an authenticated user without permission to access a data source can retrieve its connection details and credentials. Successful exploitation exposes sensitive data source information and may enable unauthorized access to the underlying databases using the disclosed credentials. This issue affects Apache DolphinScheduler: before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	7.1	More Details
CVE-2026-42697	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Inisev Social Share Icons & Social Share Buttons ultimate-social-media-plus allows Reflected XSS.This issue affects Social Share Icons & Social Share Buttons: from n/a through 3.7.5.	7.1	More Details
CVE-2026-108693	ImageMagick on Windows through 7.1.2-33 and 6.9.13-58 contains an uncontrolled search path vulnerability in NTGhostsriptEXE() that launches gswin64c.exe by bare name when Ghostscript is unregistered. Attackers can plant a malicious gswin64c.exe in the working directory to execute code with ImageMagick privileges when PDF, PostScript, or EPS files are converted.	7.0	More Details
CVE-2026-19574	The ARM64 MMU back-end allocated address space identifiers (ASIDs) for memory domains with a bare round-robin counter in arch_mem_domain_init() (arch/arm64/core/mmu.c). VM_ASID_BITS is 8, so only 255 ASIDs exist; once the counter wrapped, arch_mem_domain_init() could hand an ASID to a new domain while a still-live domain held the same one. Domain-private mappings are installed non-global (MT_NG), so the ASID is the only tag separating one domain's cached translations from another's in the TLB. The context-switch path in z_arm64_swap_ptables() only flushes the TLB when the outgoing and incoming domains carry the same ASID, which does not cover a duplicate reached through a third domain: for domains A and C sharing an ASID and an unrelated domain B, the schedule A -> B -> C never takes the flush branch, so the ASID-tagged entries A populated remain resident while C runs. Under SMP two live domains sharing an ASID can additionally be resident on two CPUs at once, which the architecture does not allow for distinct translation-table sets. Triggering the wrap requires a CONFIG_USERSPACE application on ARM64 that creates more than 255 memory domains over its lifetime; k_mem_domain_init() and k_mem_domain_deinit() are supervisor-only APIs and are not exposed as syscalls, so an unprivileged thread cannot drive the counter directly. Once two live domains alias, however, a user-mode thread in one domain can read and write memory belonging to the other domain's partitions and thread stacks with that domain's permissions, defeating the memory-domain isolation boundary. The fix scans the live domain_list before assigning an ASID, advances the round-robin counter past ASIDs already in use, and returns -ENOMEM when all are taken, so domain creation fails closed instead of silently aliasing.	7.0	More Details
CVE-2026-108744	pbi-cli 3.10.1 through 3.12.0 contains an OS command injection vulnerability in desktop_sync.py that passes unquoted .pbip paths to cmd /c start when reopening projects. Attackers can lure victims into opening a Power BI project from a space-free path containing & to run commands with victim privileges during report write or reload.	7.0	More Details
CVE-2026-78022	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Not Failing Securely ('Failing Open') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	6.8	More Details
CVE-2025-14123	The Redux Framework plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 4.5.11. This is due to the plugin saving arbitrary meta keys under a registered option name without sufficient capability checks or key allowlist / restrictions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to set an arbitrary role (e.g., Administrator) when performing a profile update if a plugin or theme using this framework has added at least one user profile field that leverages Redux_Users::set_profile/set_section/set_field.	6.8	More Details
CVE-2026-108759	mistral.rs 0.9.0 through 0.9.4 contains a link following vulnerability in mistralrs-code-exec that allows sandboxed shell code to read and overwrite files outside the sandbox via symlinks. Attackers or prompt-injected agents can name symlinks as outputs or reuse sessions with symlinked input paths to access files with the server process's permissions.	6.8	More Details
CVE-2026-	The Mechanize library is used for automating interaction with websites. Prior to 2.14.1, Mechanize sends caller-supplied credential headers to a different host after an HTTP redirect. Mechanize#request_headers= is reapplied by Mechanize::HTTP::Agent#request_add_headers even after Mechanize::HTTP::Agent#response_redirect strips per-request headers, and the protected header lists omit	6.8	More Details

107715	Proxy-Authorization and Cookie2. An attacker who controls a redirect target can capture bearer tokens or session cookies supplied through request_headers= or the per-request headers argument, while Mechanize#cookie_jar and Mechanize::HTTP::AuthStore are not affected. This issue is fixed in version 2.14.1.		
CVE-2026-104652	The Envira Gallery WordPress plugin before 1.16.1 does not sanitise and escape a gallery item identifier before outputting it in an image tag attribute, allowing users with the Author role and above to inject arbitrary web scripts that execute when any visitor, including an administrator, views a page embedding the gallery.	6.8	More Details
CVE-2026-104653	The Envira Gallery WordPress plugin before 1.16.1 does not sanitise or escape user-supplied gallery display configuration values before storing them and outputting them in an image tag attribute, allowing users with the Author role and above to inject arbitrary web scripts that execute when any visitor, including an administrator, views a page containing the affected gallery.	6.8	More Details
CVE-2026-104667	The Animated Number Counters WordPress plugin before 3.1 does not sanitise or escape a value stored by an Editor-level user before concatenating it into a SQL query that runs when any unauthenticated visitor renders a page containing the counter, leading to second-order SQL injection that can read arbitrary data including password hashes.	6.8	More Details
CVE-2026-104953	The MPG WordPress plugin before 4.2.3 does not properly validate the structure of imported project data before using it in a database query, allowing users with the Editor role or higher to perform SQL injection attacks and read sensitive data such as password hashes.	6.8	More Details
CVE-2026-109082	A flaw was found in the Client-Initiated Backchannel Authentication CIBA implementation within the keycloak-services component of Keycloak. This component handles advanced authentication flows where a client initiates a login on behalf of a user. The issue occurs because Keycloak fails to verify that a client is authorized to use the CIBA flow, allowing public clients to bypass security requirements. An attacker could use this flaw to trick a user into approving a login request, eventually gaining full access to the users account without needing a client secret.	6.8	More Details
CVE-2026-19576	The Goodix GT9xx input driver in drivers/input/input_gt911.c reads the touch point count from the controller's status register and masks it with GT911_TOUCH_POINTS_MSK (0x0F), yielding a value of 0..15. In gt911_process() that value is used directly as the loop bound for filling point_reg[], a stack array sized to CONFIG_INPUT_GT911_MAX_TOUCH_POINTS, whose Kconfig range is 1..5 with a default of 1. No other check constrains the count; the driver relied only on a comment asserting that the controller had been programmed at init to report no more points than configured. Each loop iteration issues an I2C read of eight bytes straight into point_reg[i], so a controller that reports more points than the array holds causes up to 112 bytes of peer-supplied data to be written past the end of the array, over the stack frame of gt911_process() in the system workqueue thread. Two further loops then read out of bounds from the same array. Triggering it requires control of, or the ability to substitute, the I2C touch controller — plausible on the many supported boards where the GT9xx panel is a pluggable display module or shield rather than an on-PCB part; a spoofed device need only answer the init probes with a supported product ID and a checksum-valid config blob. The same overflow can also occur non-adversarially, with a GT9271-class panel that ignores the driver's touch-count programming and reports up to ten points, or with bus corruption of the single status byte. The impact is an out-of-bounds stack write with fully attacker-chosen content executing at kernel privilege, i.e. potential control-flow hijack on the host MCU, in addition to out-of-bounds reads and crashes. The attack vector is physical/local hardware access only; there is no network, USB, or syscall path to the defect. The fix clamps the reported count with min() against CONFIG_INPUT_GT911_MAX_TOUCH_POINTS before any array indexing.	6.8	More Details
CVE-2026-107162	Express Gateway through 1.16.11 contains an authentication bypass vulnerability in the OAuth 2.0 refresh_token grant that fails to validate the token secret or issuing client. Attackers with any valid client credentials and the identifier portion of another user's refresh token can obtain that user's access token and impersonate them against oauth2-protected APIs.	6.8	More Details
CVE-2026-12980	The Post Snippets WordPress plugin through 4.2.4 does not properly escape variable values substituted into snippets before outputting them, allowing users with the Contributor role and above to inject arbitrary web scripts that execute when the content is viewed.	6.8	More Details
CVE-2026-107394	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to 3.3.13, the previous fix for CVE-2026-25738 did not cover an edge case, allowing an event organizer to submit a crafted URL that points to a prohibited local target but is accepted as valid by Indico. The organizer can read data returned by the target through affected Indico features. This issue is fixed in version 3.3.13.	6.8	More Details
CVE-2026-108737	Traccar through 6.16.0 contains a weak password recovery vulnerability that allows attackers to reuse password reset tokens as session credentials because TokenManager does not bind tokens to a purpose. Attackers holding a leaked reset link can obtain a full session via /api/session or change passwords via /api/password/update, retaining access for seven days even after the victim resets their password.	6.8	More Details
CVE-2026-81156	The Robo Gallery WordPress plugin before 5.2.6 does not sanitise and escape some of its gallery settings before outputting them on the gallery edit screen, allowing users with the Contributor role and above to store JavaScript that executes in the context of an administrator who opens the gallery for editing.	6.8	More Details

CVE-2026-81155	The Robo Gallery WordPress plugin before 5.2.6 does not sanitise and escape a gallery setting before outputting it on a frontend page, allowing users with the Author role and above to perform Stored Cross-Site Scripting attacks that execute in the browser of any visitor viewing a gallery, including administrators.	6.8	More Details
CVE-2026-66481	Author Arbitrary File Deletion in Presto Player Pro <= 3.0.1 versions.	6.8	More Details
CVE-2026-81153	The Robo Gallery WordPress plugin before 5.2.6 does not sanitise and escape some of its image settings before outputting them in a gallery page, allowing users with the Author role and above to perform Stored Cross-Site Scripting attacks that execute in the browser of any visitor viewing the gallery, including administrators, even where the unfiltered_html capability is disallowed such as on multisite.	6.8	More Details
CVE-2026-106097	The Code Snippets WordPress plugin before 3.10.0 does not sanitise and escape a user-supplied parameter before using it in a SQL query in some of its snippet-migration import endpoints, which are accessible to any user holding site-administration capabilities; on a WordPress Multisite network those belong to subsite Administrators, allowing a subsite Administrator who is not a network Super Admin to perform UNION-based SQL injection against shared network tables and disclose network-wide data such as other users' password hashes.	6.8	More Details
CVE-2026-81154	The Robo Gallery WordPress plugin before 5.2.6 does not sanitise and escape image alt text before outputting it in one of its gallery layouts, allowing users with the Author role and above to perform Stored Cross-Site Scripting attacks that execute in the browser of any user viewing the affected gallery, including administrators.	6.8	More Details
CVE-2026-105269	Satel Netco Design versions prior to v2.1.7 contains a stored cross site scripting vulnerability. An authenticated user with Network Operator privileges could store untrusted content that is rendered without adequate neutralization. Successful exploitation could allow script execution in another user's browser when the affected content is viewed.	6.8	More Details
CVE-2026-104898	The Online Scheduling and Appointment Booking System - Bookly plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 28.4 via the 'id, wp_user_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the WordPress account binding of any Bookly staff record, including those owned by administrators, effectively hijacking a higher-privileged staff member's account association and escalating privileges. Exploitation requires the attacking user to be linked to at least one Bookly staff record, which occurs by default whenever an admin enables the bookly_gen_allow_staff_edit_profile option (active on fresh installs) and links a WordPress user to a staff entry.	6.8	More Details
CVE-2026-89235	The Testimonials by BestWebSoft WordPress plugin through 1.0.8 does not sanitise and escape a parameter before using it in a SQL query, allowing unauthenticated attackers to append additional SQL to the query.	6.8	More Details
CVE-2026-108110	MOVO through 0.2.3 contains an authorization bypass vulnerability in the chat-api document endpoints that allows authenticated users to access other users' stored objects by supplying arbitrary object paths. Attackers who know a target's object path can send it to /api/documents/fetch or /api/documents/save-blueprint to read private documents and overwrite presentation blueprints.	6.8	More Details
CVE-2026-107176	A flaw was found in the cluster-samples-operator. The RBAC Role coreos-pull-secret-reader in namespace openshift-config grants get, list, and watch permissions on all Secret resources without resourceNames scoping. The operator only requires access to the pull-secret Secret. If the samples-operator pod or its service account token is compromised through a separate vulnerability, an attacker could read all secrets in openshift-config, potentially including OAuth identity provider credentials, cloud provider credentials, and other sensitive cluster configuration.	6.8	More Details
CVE-2026-107228	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. From 2.1.0 until 3.0.14, the enabled-by-default cookie store replaces a Cookie header explicitly supplied through setHeader or addHeader whenever the store contributes any cookie for the origin. In a shared client, stored cookies originating from one user can replace a different user's request cookie, causing the request to execute under the wrong session. This bypasses the earlier CVE-2024-53990 remediation, which covered cookies supplied through addCookie but not a directly supplied header. This issue is fixed in version 3.0.14.	6.8	More Details
CVE-2026-107399	The Mechanize library is used for automating interaction with websites. Prior to 2.14.1, Mechanize applies no origin trust boundary in Mechanize::HTTP::Agent#response_follow_meta_refresh when Mechanize#follow_meta_refresh is enabled. A page containing a meta refresh to another origin causes headers configured through Mechanize#request_headers= to be reapplied to the refresh request, allowing an attacker who controls content in the crawl to capture bearer tokens or session cookies. The default configuration is not affected because follow_meta_refresh is false, and the exposure is limited to caller-supplied default headers. This issue is fixed in version 2.14.1.	6.8	More Details

CVE-2026-89191	Unsanitised input in the "template name" field of SQLView KRIS's Workflow Template feature is rendered in "onclick" attributes on the main dashboard without proper server-side sanitisation, allowing an attacker with administrative access to inject and store malicious scripts that execute in the browsers of affected users.	6.8	More Details
CVE-2026-107638	pH7Builder (pH7 Social Dating CMS) before 18.5.0 contains an improper restriction of authentication attempts vulnerability that allows attackers to bypass two-factor authentication by guessing TOTP codes without limits. Attackers who know an account password can submit unlimited 6-digit verification codes to VerificationCodeFormProcess.php to take over member, affiliate, or administrator accounts.	6.8	More Details
CVE-2026-107275	@fastify/jwt is a JSON Web Token plugin for the Fastify web framework. In versions before 10.2.3, a time span passed to expiresIn, notBefore, or maxAge that the plugin's parser cannot read, such as a compound span, a month unit, an ISO 8601 duration, a decimal comma, or a value with surrounding whitespace, is silently dropped instead of refused. On the signing path this produces a token with no expiration claim that never expires, and on the verification path a configured maxAge stops being enforced, so a token that should be rejected for age is accepted. The issue is fixed in @fastify/jwt 10.2.3, and users should upgrade to 10.2.3 or later. As a workaround, pass these options as a number of seconds, or verify that any time-span string parses to a finite value before relying on it.	6.8	More Details
CVE-2026-107446	containerd overlaybd through 1.0.18 has a do_load_index (LSMT index loading) integer overflow (and resultant out-of-bounds heap access) for index_bytes, if an untrusted overlaybd blob from a registry is used in a scenario with multiple overlaybd-backed containers.	6.8	More Details
CVE-2026-107323	The Gallery PhotoBlocks WordPress plugin before 1.3.6 does not sanitize and escape one of its gallery settings before outputting it into an HTML attribute, allowing users with Contributor-level access and above to store JavaScript that executes in the browser of anyone who views a page containing the gallery, including administrators.	6.8	More Details
CVE-2026-104646	The Image Photo Gallery Final Tiles Grid WordPress plugin before 3.6.14 does not sanitise several gallery configuration values that can be overridden through its gallery shortcode before printing them into an inline script block, allowing users with contributor-level access and above to inject arbitrary JavaScript that executes in the session of anyone viewing the post, including an administrator previewing a pending submission. No gallery ownership is required: any gallery that already exists on the site can be referenced.	6.8	More Details
CVE-2026-107289	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.56.0 until 1.107.6 and 2.44.0, applications that opt attacker-influenced URLs into local network access through FileUrl with force_download='allow-local' or web_fetch_tool with allow_local_urls=True can bypass the cloud-metadata blocklist by appending an IPv6 zone identifier to an IPv6 metadata address. IPv6Address equality and hashing include the zone identifier, so the blocklist comparison fails even though the network stack ignores the zone on a non-link-local destination and reaches the metadata service, potentially exposing cloud IAM credentials. The opt-in settings are disabled by default, and the issue requires an IPv6-enabled environment. This issue is fixed in versions 1.107.6 and 2.44.0.	6.8	More Details
CVE-2026-19571	The ITE IT8xxx2 SHI host-command backend (subsys/mgmt/ec_host_cmd/backends/ec_host_cmd_backend_shi_ite.c) copied the 8-byte host-command request header from the SPI Rx FIFO directly into the shared receive buffer data->in_msg and only afterwards checked the protocol version and the derived packet length. The interrupt handler also accepted a chip-select assertion and an Rx-valid-length (RVLI) interrupt in any driver state other than SHI_STATE_DISABLED, so a new header could be parsed while the host-command thread was still processing the previous request out of the very same buffer. The host processor is the SPI controller and drives both chip select and the clock. After sending a well-formed request it can immediately de-assert chip select — which returns the driver to the ready state and re-enables the FIFO — and start a second transaction carrying a header with data_len = 0xFFFF. Those eight bytes are written into in_msg before the oversized length is rejected, so they land in a buffer whose contents verify_rx() in subsys/mgmt/ec_host_cmd/ec_host_cmd_handler.c has already validated. If this lands in the window before the host-command thread executes args.input_buf_size = rx_header->data_len, the framework hands the registered command handler a 65535-byte input length over a 256-byte buffer. The result is an out-of-bounds read of up to roughly 64 KiB beyond the request buffer: command handlers that copy or echo input_buf_size bytes disclose adjacent embedded-controller memory back to the host or overflow the response buffer, and a read past the end of SRAM faults the controller. The same race also allows cmd_id and cmd_ver to be swapped after checksum verification and after handler lookup. Exploitation requires the ability to drive the inter-processor SHI bus (a compromised host OS or physical access to the SPI lines) and winning a timing race, which the SPI controller can retry indefinitely. The fix parses the header into a local struct ec_host_cmd_request_header and copies it into in_msg only after the length has been bounded by sizeof(data->in_msg), and ignores chip-select and RVLI interrupts outside SHI_STATE_READY_TO_RECV/SHI_STATE_RECEIVING. A residual, bounded race remains: an end-of-transaction interrupt still resets the state to ready while the host-command thread owns the buffer, so a valid second request can still overwrite the in-flight request's contents, unlike the NPCX backend which parks in SHI_STATE_CNL_RESP_NOT_RDY while the buffer is in use.	6.7	More Details
	Improper link resolution and external control of file paths in the administrative command-line operations of hMailServer.exe in Progressive Robot hMailServer 6.3.4 and 6.3.5 allow a local attacker who already runs code as the low-privilege service account to escalate privilege. On Windows, operations run with		

CVE-2026-107578	administrator rights by the installer, DBSetup, the Control Panel or an administrator wrote log entries and crash records into the log folder, created, deleted and changed the permissions of the self-signed certificate and private key in the data folder, and rewrote message files in the data folder, all by path in folders the service account (NT SERVICE\hMailServer, the default for new installations since 6.3.4) can modify, following junctions and mount points; and the store-maintenance operations reached files by names taken from the database, which the service account can write, including names outside the data folder. On Linux, the store-maintenance and object-storage operations run as root followed symbolic links the service account (the packaged hmailserver user, which owns the data folder) planted in it, so a root-run operation read, wrote or removed the link's target as root. A local attacker controlling the service account can thereby gain the administrator's (Windows) or root's (Linux) privileges when such an operation is run.	6.7	More Details
CVE-2026-86828	The BackWPup WordPress plugin before 5.7.7 does not properly restrict the destination path of files extracted during a backup restore when its fallback archive library is used, allowing high-privileged users to write files outside the intended restore directory, potentially leading to remote code execution.	6.6	More Details
CVE-2026-107427	Authorization Bypass Through User-Controlled Key vulnerability in NOUS Ouvert Utile et Simple Event post event-post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event post: from n/a through 6.1.1.	6.5	More Details
CVE-2026-109080	SQL injection in the bulk license plate search of the Flock Night Shift hosted service allowed an authenticated user to read other customer organizations' data, including license plate recognition records, via a crafted license plate value. Data could not be modified. Flock identified the issue through internal security review and remediated it on 2026-08-12; no customer action is required.	6.5	More Details
CVE-2026-108812	A security vulnerability has been detected in SEMCMS up to 5.0. The impacted element is an unknown function of the file /admin/SEMCMS_User.php?Class=Deleted&CF=user. Such manipulation leads to improper authorization. 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.	6.5	More Details
CVE-2026-107193	A flaw has been found in **permission filters** in the **foreman** package. The API loads a filter by its identifier and does not apply the search limit on the caller's permission. A low-privileged network attacker or user must already be allowed to delete filters for one role only. They can delete filters that belong to other unlocked roles. Those other roles then lose the access the deleted filters had granted.	6.5	More Details
CVE-2026-107791	The WP Comment Cleaner WordPress plugin before 7.2 does not perform a capability check or validate a nonce on one of its bulk comment-deletion routines, allowing authenticated users with minimal permissions, such as subscribers, to permanently delete all comments on the site.	6.5	More Details
CVE-2026-107864	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Igor Funa Ad Inserter ad-inserter allows Stored XSS.This issue affects Ad Inserter: from n/a through 2.8.18.	6.5	More Details
CVE-2026-108784	A vulnerability was detected in macrozheng mall up to 1.0.3. This vulnerability affects the function AlipayServiceImpl.pay of the file com/macro/mall/portal/service/impl/AlipayServiceImpl.java of the component Payment Endpoint. The manipulation of the argument total_amount results in business logic errors. The attack can be launched remotely. The exploit is now public and may be used. The patch is identified as dcaa93b3150352e5044708d7211b5bed0af4509f. A patch should be applied to remediate this issue.	6.5	More Details
CVE-2026-19740	The Link Layer Control Procedure (LLCP) implementation of the Zephyr software Bluetooth LE Controller retains the receive node that carried an accepted LL_PHY_UPDATE_IND so that it can later be reused for the host notification when the update instant is reached (llcp_rx_node_retain() in subsys/bluetooth/controller/ll_sw/ull_llcp.c, and the node is deliberately not recycled while marked NODE_RX_TYPE_RETAIN). The invalid-PDU arms of llcp_lp_pu_rx() and llcp_rp_pu_rx() in subsys/bluetooth/controller/ll_sw/ull_llcp_phy.c completed the procedure via llcp_lr_complete() / llcp_rr_complete() without first releasing that retained node, so the procedure context — the only remaining reference to the node — was freed while the node was still held out of the receive pool. A peer device on an established LE connection can drive this deterministically and without pairing or encryption. Against a peripheral it sends LL_PHY_REQ, receives LL_PHY_RSP, sends a valid LL_PHY_UPDATE_IND with an instant a few connection events in the future (so the node becomes retained), and then, before the instant is reached, sends any other LL Control PDU such as LL_LENGTH_REQ; ull_cp_rx() routes it to the active remote PHY Update procedure, which takes the invalid-PDU path. The mirror case applies to a locally initiated PHY Update followed by an LL_REJECT_IND. In the default configuration (CONFIG_BT_ASSERT and CONFIG_BT_CTLR_ASSERT_DEBUG both default y) the violated invariant in llcp_lr_check_done() / llcp_rr_check_done() triggers a controller assertion, ending in k_oops() (or k_panic()) — a single crafted PDU sequence from radio range faults the device. With those assertions compiled out, each attempt silently leaks one receive PDU node and its memq link; because the controller receive pool is small (PDU_RX_CNT, driven by CONFIG_BT_CTLR_RX_BUFFERS, which defaults to 1) and each attempt costs the attacker only a reconnect, a few repetitions exhaust the pool and leave Bluetooth inoperable until reboot. On releases v3.4.0 through v3.7.x the assertion is never reached, whatever the configuration, so every attempt leaks silently. The impact is limited to availability: the orphaned node leaves no dangling pointer that is later dereferenced and is never delivered to the host, so there is no memory corruption or information disclosure. The same pull request applies the identical release to the Connection Update and CIS-create procedures, whose invalid-PDU	6.5	More Details

	arms had the same omission.		
CVE-2026-19739	The Bluetooth Link Layer control procedure code in <code>subsys/bluetooth/controller/ll_sw/ull_llcp_conn_upd.c</code> retains the received RX node while a Connection Update / Connection Parameter procedure waits for its instant, so the node can later carry the host notification (<code>llcp_rx_node_retain()</code>), which marks it <code>NODE_RX_TYPE_RETAIN</code> and thereby suppresses the normal recycling in <code>ull.c</code>). The default: arm of <code>llcp_rp_cu_rx()</code> and <code>llcp_lp_cu_rx()</code> — the "invalid PDU, terminate the connection" path — completed the procedure without releasing that retained node. <code>llcp_rr_check_done()</code> then dequeued and freed the procedure context with <code>ctx->node_ref.rx</code> still pointing at the retained node, dropping the last reference to it. A peer device in radio range can reach this without pairing, bonding, or encryption. Against a peripheral, the peer sends a well-formed <code>LL_CONNECTION_UPDATE_IND</code> with an instant a few connection events in the future (the node is retained and the procedure enters <code>RP_CU_STATE_WAIT_INSTANT</code>), then, before the instant is reached, sends any other LL Control PDU such as <code>LL_LENGTH_REQ</code>. <code>ull_cp_rx()</code> routes that PDU into the active remote Connection Update procedure, which takes the invalid-PDU path. The central role is reachable symmetrically after accepting an <code>LL_CONNECTION_PARAM_REQ</code>, and the local-procedure variant is reachable with <code>LL_REJECT_IND</code>. With <code>CONFIG_BT_CTLR_ASSERT_DEBUG</code> enabled (its default), the resulting state violates the invariant asserted in <code>llcp_rr_check_done()</code>, so the two-PDU sequence produces an immediate fatal error in the controller. With those asserts disabled, each occurrence permanently loses one node from the controller's small fixed RX pool (sized from <code>CONFIG_BT_CTLR_RX_BUFFERS</code>, which defaults to 1); repeating the sequence across reconnections exhausts the pool, after which the link-layer receive path operates on a NULL node. The impact is an unauthenticated, remotely triggerable denial of service persisting until reboot; there is no memory-disclosure or memory-corruption consequence, since the leaked node simply becomes unreachable.	6.5	More Details
CVE-2026-19738	The Bluetooth Link Layer Control Procedure (LLCP) implementation for Connected Isochronous Stream (CIS) creation retains an RX node (<code>ctx->node_ref.rx</code>, marked <code>NODE_RX_TYPE_RETAIN</code>) so it can later be reused as the host notification — on the peripheral while awaiting the Host's reply to an <code>LL_CIS_REQ</code>, and on the central for the whole duration of a locally initiated CIS Create. In <code>subsys/bluetooth/controller/ll_sw/ull_llcp_cc.c</code>, the "invalid PDU received" paths of <code>llcp_rp_cc_rx()</code> and <code>llcp_lp_cc_rx()</code> terminated the connection and completed the procedure without releasing that retained node, breaking the invariant checked in <code>llcp_lr_check_done()</code> and <code>llcp_rr_check_done()</code> and orphaning the node's memory. A peer device within radio range can reach this with a single extra LL Control PDU on an unauthenticated, unencrypted ACL link. Against a peripheral, the attacker sends a valid <code>LL_CIS_REQ</code> and then, before the Host replies, any unrelated LL Control PDU (for example <code>LL_VERSION_IND</code>), which <code>ull_cp_rx()</code> routes into the active remote procedure. Against a central performing a CIS Create, a malicious peripheral answers with <code>LL_UNKNOWN_RSP</code> for <code>CIS_REQ</code>, which is dispatched into the active local procedure. No pairing, encryption or user interaction is required; the code is compiled in when <code>CONFIG_BT_CTLR_PERIPHERAL_ISO</code> or <code>CONFIG_BT_CTLR_CENTRAL_ISO</code> is enabled. In default builds (<code>CONFIG_BT_CTLR_ASSERT_DEBUG</code> is default y) the retained-node assertion fires immediately, producing a controller fatal error and, typically, a system reset from one injected PDU. With the development assertions disabled, each attempt permanently loses one node from the controller's small LL notification pool (<code>LL_PDU_RX_CNT</code>, <code>2 * CONFIG_BT_CTLR_LLCP_CONN</code>) together with its <code>memq_link_t</code>; repeating the connect-attack-reconnect cycle exhausts the pool, after which notification allocation always fails, RX flow control stalls, and the non-disableable <code>LL_ASSERT_ERR()</code> in <code>llcp_lp_cc_flush()</code> faults. The impact is limited to availability — the leaked node is orphaned, never reused or double-freed — and recovery requires a reboot.	6.5	More Details
CVE-2026-104915	The Academy LMS – AI Course Builder, Quizzes, Certificates & eLearning plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.0.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with custom-level access and above, to permanently delete arbitrary Academy lesson comments and their replies authored by any user, including administrators, across courses they do not instruct. This is exploitable by any user registered as an Academy instructor for at least one course, as they can supply their own <code>course_id</code> to pass the instructor check while targeting comments belonging to entirely different courses.	6.5	More Details
CVE-2023-25996	Insertion of Sensitive Information Into Sent Data vulnerability in Pluggabl LLC. Booster Elite for WooCommerce booster-elite-for-woocommerce allows Retrieve Embedded Sensitive Data.This issue affects Booster Elite for WooCommerce: from n/a before 8.4.0.	6.5	More Details
CVE-2026-62049	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetBlocks For Elementor jet-blocks allows Stored XSS.This issue affects JetBlocks For Elementor: from n/a through 1.5.2.1.	6.5	More Details
CVE-2026-107865	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetMenu jet-menu allows Stored XSS.This issue affects JetMenu: from n/a through 3.0.5.	6.5	More Details
CVE-2026-109168	lamp-cloud through 5.10.1 contains an insecure direct object reference vulnerability that allows authenticated users to list other business objects' file attachments by supplying an arbitrary <code>bizId</code> to the <code>listFileByBizId</code> endpoint. Attackers can retrieve file names, storage paths, MD5 hashes and stored URLs, which in default LOCAL storage are served without login under <code>/anyTenant/file</code>.	6.5	More Details
CVE-2026-	HortusFox (hortusfox-web) before 6.2 contains an SQL injection vulnerability that allows API token holders to inject SQL by supplying crafted <code>include_info</code> values to the <code>/api/locations/list</code> endpoint. Attackers can place	6.5	More

108100	subqueries in include_info, which PlantsModel::getSpecificInfo() concatenates into the column list, to read any database table including user password hashes.		Details
CVE-2026-107717	Banks generates meaningful LLM prompts using a simple template language. Prior to 2.5.0, Banks Prompt.chat_messages() attempts to parse every line of rendered template output as ChatMessage JSON. When an application renders untrusted data and passes the returned ChatMessage objects to an LLM provider, attacker-controlled JSON can cross the prompt boundary and become a system, assistant, or tool message because ChatMessage.role accepts arbitrary strings. This can override application instructions, alter the intended prompt structure, or confuse downstream tool and message handling. This issue is fixed in version 2.5.0.	6.5	More Details
CVE-2026-109169	LogicalDOC Community Edition through 9.3 contains a sql injection vulnerability that allows authenticated users to execute crafted SQL via the firstLetter parameter of TagsDataServlet. Low-privileged attackers can inject UNION SELECT statements returned in the XML tag list to read usernames, email addresses and password hashes from Id_user.	6.5	More Details
CVE-2026-93693	In Progress ShareFile Storage Zones Controller v5.12.6 and below, improper validation of outbound request destinations and parameters, unsafe JSONP response formatting, and insufficient validation on queue service can be chained by a remote unauthenticated attacker to issue server-side requests to unintended local handlers and perform unauthorized queue operations.	6.5	More Details
CVE-2026-109187	jshERP through 3.6 contains an information disclosure vulnerability that allows any authenticated user to read platform-wide configuration secrets via the getInfoByKey handler of PlatformConfigController. Low-privilege users of any tenant can request arbitrary platformKey values such as email_auth_code or activation_code to obtain SMTP authorization codes and activation secrets, because only aliOss and weixin keys are blocked.	6.5	More Details
CVE-2026-109174	MoguBlog through 6.2 contains an information disclosure vulnerability that allows low-privileged front-end users to read system credentials via the getSystemConfig endpoint. Attackers can supply an ordinary reader session token to retrieve unfiltered SystemConfig data, exposing Qiniu and MinIO secret keys and SMTP mailbox passwords.	6.5	More Details
CVE-2026-107828	JiveJdon through 5.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to access Weibo-created accounts by deriving predictable credentials from public Weibo user IDs. OAuthAccountServiceImp.transferSina() sets the password to the first four digits of the Weibo ID, letting attackers log in through normal form login to read or post as victims.	6.5	More Details
CVE-2026-109166	lamp-cloud through 5.10.1 contains an insecure direct object reference vulnerability that allows authenticated users to obtain storage URLs for other users' files by supplying arbitrary file ids. Attackers can send another user's file ids to the findUrlById handler of FileAnyoneController, which never checks ownership, to retrieve access URLs and read uploaded attachments.	6.5	More Details
CVE-2026-86851	The Liveees Checkout WordPress plugin through 7.0.2 does not perform any capability, nonce or order-key check before acting on request parameters on the order confirmation page, allowing unauthenticated users to change the status of arbitrary orders, store arbitrary data and notes on them, and recover their order keys.	6.5	More Details
CVE-2026-62029	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFunnels Team WPFunnels wpfunnels allows Stored XSS.This issue affects WPFunnels: from n/a through 3.13.3.	6.5	More Details
CVE-2026-108951	LavaLite CMS through 10.1.2 contains an authorization bypass vulnerability that allows authenticated low-privileged users to modify other users' accounts by abusing the AbstractRequest isWorkflow() check. Attackers can send a PATCH request to the user update route with a target identifier to change name, email, password, status, or mobile, including for administrators.	6.5	More Details
CVE-2026-108158	plugNmeet Server through 2.5.2 contains a path traversal vulnerability in the whiteboard conversion endpoint that allows any meeting participant to read server files via crafted filePath values. Attackers can supply ../ sequences so text or office documents are converted into page images, then fetch them unauthenticated through /download/uploadedFile/.	6.5	More Details
CVE-2026-42695	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FolioVision FV Flowplayer Video Player fv-wordpress-flowplayer allows Stored XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.54.7212.	6.5	More Details
CVE-2026-48484	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev101, the API `rpc` function in `api_blueprint.py` handles `multipart/form-data` uploads by reading the whole content of the uploaded file into memory with `file.read()`. This occurs before the data is sent to the underlying function. Since there is no size limit set at this point, a large file upload can exhaust the server's available memory which led to process termination. Version 0.5.0b3.dev101 contains a patch.	6.5	More Details
	Improper authorization in the query resolvers generated by @aws-amplify/graphql-index-transformer in AWS Amplify API Category before 3.1.2 might allow an authenticated remote user to read records owned by other		

CVE-2026-108096	users of the same application via crafted queries. This issue has been addressed in @aws-amplify/graphql-index-transformer 3.1.2 https://www.npmjs.com/package/@aws-amplify/graphql-index-transformer/v/3.1.2 (included in @aws-amplify/data-construct 1.17.4 https://www.npmjs.com/package/@aws-amplify/data-construct/v/1.17.4 and @aws-amplify/graphql-api-construct 1.21.4 https://www.npmjs.com/package/@aws-amplify/graphql-api-construct/v/1.21.4). We recommend upgrading to the latest version ensuring any forked or derivative code is patched to incorporate the new fixes and then redeploying their backend.	6.5	More Details
CVE-2026-108168	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DLX Plugins Custom Query Blocks post-type-archive-mapping allows Stored XSS.This issue affects Custom Query Blocks: from n/a through 5.6.0.	6.5	More Details
CVE-2026-107866	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor jet-elements allows Stored XSS.This issue affects JetElements For Elementor: from n/a through 2.9.2.3.	6.5	More Details
CVE-2026-62039	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Html5 Audio Player html5-audio-player allows Stored XSS.This issue affects Html5 Audio Player: from n/a through 2.8.8.	6.5	More Details
CVE-2026-108904	pH7Builder (pH7 Social Dating CMS) before 18.5.0 contains an information disclosure vulnerability that allows API clients to obtain sensitive member data because UserController::users() and user() return unfiltered database rows. Attackers holding a valid private API key can retrieve bcrypt password hashes, non-expiring hashValidation reset tokens, and TOTP secrets to take over accounts and bypass two-factor authentication.	6.5	More Details
CVE-2026-108671	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to read MCP server configurations because the queryById permission check is commented out. Attackers can obtain record ids from the unguarded /airag/app/queryById endpoint and retrieve MCP endpoint URLs, headers, and outbound authentication tokens.	6.5	More Details
CVE-2026-108581	TencentCloud Octop through 1.0.2b6 contains a missing authorization vulnerability that allows authenticated low-privileged users to read stored provider API keys via GET /api/providers and GET /api/voice/providers. Attackers can query these endpoints, which only validate the JWT, to obtain plaintext LLM and voice provider API keys and abuse the upstream provider accounts.	6.5	More Details
CVE-2026-108700	1Panel-dev CordysCRM before 1.9.2 contains a missing authorization vulnerability that allows authenticated users to list business titles by calling POST /field/source/business-title without permission checks. Users lacking CONTRACT_BUSINESS_TITLE_READ can retrieve organization invoicing entities, exposing tax identification numbers, bank account numbers, opening banks, registration addresses, and phone numbers.	6.5	More Details
CVE-2026-108694	ConvertX through 0.19.0 contains an arbitrary file read vulnerability that allows authenticated users to read server files because src/converters/pandoc.ts invokes Pandoc without the --sandbox flag. Attackers can upload a reStructuredText document with an include directive naming an absolute path, convert it, and download output containing the referenced file's contents.	6.5	More Details
CVE-2026-95597	Missing Authorization vulnerability in codemstory pgall-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects : from n/a through 5.5.17.	6.5	More Details
CVE-2026-94590	Improper Verification of Source of a Communication Channel vulnerability in CodePeople2 Sell Downloads sell-downloads allows Exploitation of Trusted Credentials.This issue affects Sell Downloads: from n/a through 1.2.3.	6.5	More Details
CVE-2026-108692	1Panel-dev CordysCRM from 1.9.0 before 1.9.2 contains a missing authorization vulnerability in eight ModuleFieldController /field/source data-source endpoints lacking permission checks. Authenticated users denied module permission can page through organization-wide leads, contacts, quotations, contracts, payment plans, payment records, orders and invoices owned by other users.	6.5	More Details
CVE-2026-108677	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in GET /sys/api/getUserByName that allows low-privileged authenticated users to retrieve any user's stored password value. Attackers can decrypt the AES-CBC protected response using the hard-coded key exposed by /sys/getEncryptedString to obtain administrators' password ciphertexts for offline guessing.	6.5	More Details
CVE-2026-108661	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to transfer tenant ownership via POST /sys/tenant/changeOwenUserTenant. Low-privileged attackers can supply userId and tenantId parameters to reassign any tenant's owner to a member, including themselves, and strip the legitimate owner.	6.5	More Details
CVE-2026-108883	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the editThirdAppConfig handler that allows any authenticated user to modify third-party application configurations. Low-privileged attackers can replace client id, client secret, agent id and corp id of DingTalk, WeCom or Feishu integrations to redirect directory synchronisation and messaging to attacker-controlled applications or break them.	6.5	More Details
	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the GET		

CVE-2026-108648	/sys/api/getDynamicDbSourceByCode endpoint of SystemApiController, which lacks Shiro permission or role annotations. Any authenticated low-privileged user can supply datasource codes in the dbSourceCode parameter to retrieve JDBC URLs, usernames and decrypted cleartext database passwords.	6.5	More Details
CVE-2026-95589	Missing Authorization vulnerability in Magepeople inc. Deposits and Partial Payments for WooCommerce advanced-partial-payment-or-deposit-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Deposits and Partial Payments for WooCommerce: from n/a through 4.0.1.	6.5	More Details
CVE-2026-94667	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetReviews jet-reviews allows Stored XSS.This issue affects JetReviews: from n/a through 3.1.2.	6.5	More Details
CVE-2026-40808	Subscriber Broken Access Control in Jetpack VideoPress <= 3.6 versions.	6.5	More Details
CVE-2026-97075	Missing Authorization vulnerability in WP Media WP Rocket wp-rocket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Rocket: from n/a before 3.23.5.	6.5	More Details
CVE-2026-94665	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mamunur Rashid Classified Listing classified-listing allows Stored XSS.This issue affects Classified Listing: from n/a through 6.1.2.	6.5	More Details
CVE-2026-62098	Unauthenticated Content Injection in Boutique <= 2.3.3 versions.	6.5	More Details
CVE-2026-86850	The SKU Error Fixer for WooCommerce WordPress plugin through 1.0 does not perform any capability or nonce checks on two of its AJAX actions, which are also available to unauthenticated users, allowing them to permanently delete product variations it classifies as obsolete, and to disclose those variations' details, with no recoverable copy left behind.	6.5	More Details
CVE-2026-108580	AniWorld Downloader before 5.3.0 contains an improper restriction of authentication attempts vulnerability in the WebUI /login POST handler that allows unauthenticated attackers to guess passwords without throttling. Attackers can enumerate usernames through verify_user response timing and brute-force passwords on exposed WebUI instances to take over accounts.	6.5	More Details
CVE-2026-108547	AstronRPA through 1.1.6 contains a missing tenant authorization check in robot-service that allows authenticated users to read other tenants' shared variables via the get-batch-shared-var endpoint. Attackers can enumerate sequential shared variable IDs and decrypt all-users variables re-encrypted with their own tenant key to recover other tenants' credentials in plaintext.	6.5	More Details
CVE-2026-108164	Open Source Social Network (OSSN) through 10.1 contains an insecure direct object reference vulnerability in components/OssnMessages/ossn_com.php that allows authenticated users to read other users' private message attachments. Attackers can request the /messages/attachment/{guid} route with sequential or guessed file GUIDs to retrieve attachments from private conversations without sender or recipient verification.	6.5	More Details
CVE-2026-108699	hyper-mcp through 0.8.3 contains an improper signature verification vulnerability that allows attackers to load malicious WebAssembly plugins because cosign_verify_args() accepts any signer identity and OIDC issuer by default. Attackers controlling a plugin image reference can sign a malicious image with a free Sigstore keyless certificate to execute plugins with configured host, filesystem, and environment capabilities.	6.5	More Details
CVE-2026-108698	hyper-mcp through 0.8.3 contains a signature verification bypass vulnerability in load_wasm in src/wasm/oci.rs that verifies the Cosign signature of a separately resolved tag rather than the loaded manifest. Attackers controlling registry responses for the tag can serve an unsigned malicious manifest to the loader and a signed one to Cosign, executing unsigned WebAssembly plugins with configured host capabilities.	6.5	More Details
CVE-2026-78341	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Incorrect Authorization vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges and Unauthorized access.	6.5	More Details
CVE-2026-108757	Nexting pinclaw OpenClaw channel plugin through 0.3.0 contains a missing authentication vulnerability in src/core/http-router.ts that skips the authToken check on POST /pinclaw/send. Unauthenticated attackers reaching port 18790, which binds all interfaces by default, can inject blind prompts into the user's main OpenClaw agent session as user instructions.	6.5	More Details
CVE-2026-	The Tutor LMS WordPress plugin before 4.1.1 does not verify that the posts named in its course content ordering requests belong to a course the requester manages, allowing users with instructor level access to	6.5	More

85571	reassign the parent of any post on the site, taking other instructors' course content into their own courses and making arbitrary published content unreachable.		Details
CVE-2026-108728	Flyte 2.0.1 through 2.0.51 contains a cleartext secret storage vulnerability that allows users with Pod read access to obtain secrets by reading init container environment variables. The embedded secret manager webhook writes base64-encoded FILE-mounted secret values into the SECRETS environment variable, letting principals without Secret store access decode them from the Pod spec.	6.5	More Details
CVE-2026-108710	NornicDB through 1.4.1 contains a missing authorization vulnerability that allows authenticated users to bypass per-database read restrictions on the /nornicdb/search and /nornicdb/similar endpoints. Viewer-role users allowlisted for a database but denied read can submit search queries or node IDs to retrieve node IDs, labels and full property maps.	6.5	More Details
CVE-2026-107712	The WP Booking System – Booking Calendar plugin for WordPress is vulnerable to time-based SQL Injection via the 'current_month' parameter in all versions up to, and including, 2.1.0.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is a regression vulnerability — a capability check introduced in versions 2.0.19.11–2.0.19.14 to address CVE-2024-50425 was removed in version 2.1, meaning any authenticated subscriber-level account can reach the vulnerable handler with no nonce validation required.	6.5	More Details
CVE-2026-96337	Missing Authorization vulnerability in properfraction ProfilePress wp-user-avatar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ProfilePress: from n/a through 4.17.3.	6.5	More Details
CVE-2026-97348	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.74.3 via the get_instance_css function. This makes it possible for authenticated attackers, with contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The widget's normal update()/sanitize_field_input() pipeline — which would reject non-hex color values — is bypassed entirely because the [siteorigin_widget] shortcode handler calls \$the_widget->widget() directly on the attacker-supplied decoded JSON instance.	6.5	More Details
CVE-2026-89305	The paymendo WordPress plugin through 1.1 does not properly sanitize and escape a parameter before using it in a SQL query, allowing any authenticated user to perform SQL injection attacks.	6.5	More Details
CVE-2026-89304	The paymendo WordPress plugin through 1.1 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform blind SQL injection attacks.	6.5	More Details
CVE-2026-96653	The WP Directory Kit plugin for WordPress is vulnerable to time-based SQL Injection via 'display_name' Profile Field (Second-Order) in all versions up to, and including, 1.5.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is a second-order injection: a Subscriber stores a display_name containing a single quote via their own profile, which WordPress preserves verbatim; the payload is then triggered when WdkCachedUserEditor::update_listings_user_editor() re-reads that stored value and passes it unsanitized to the SQL sink.	6.5	More Details
CVE-2026-108162	Pingvin Share X before 1.22.0 contains a rate limit bypass vulnerability that allows unauthenticated remote attackers to evade per-IP throttling because backend/src/main.ts unconditionally trusts proxy headers. Attackers can rotate spoofed X-Forwarded-For values against /api/auth/signIn, /api/auth/signIn/totp, and /api/auth/resetPassword to brute-force passwords and TOTP codes and forge logged client IP addresses.	6.5	More Details
CVE-2026-108163	Pingvin Share X before 1.22.0 contains an ineffective rate limiting vulnerability because throttler TTL values specified in seconds are interpreted as milliseconds. Unauthenticated attackers can send effectively unthrottled requests to /api/auth/signIn, /api/auth/signIn/totp and /api/auth/resetPassword to brute-force passwords and TOTP codes.	6.5	More Details
CVE-2026-107803	ProcessMaker is an open source workflow management software suite. Prior to 2026.14.3, the `GET /api/1.0/tasks` endpoint in ProcessMaker is vulnerable to SQL injection through the order_by parameter because `ProcessMaker\Traits\TaskControllerIndexMethods::applyColumnOrdering()` concatenates a user-controlled process_requests column name into a DB::raw() SQL subquery without validation or parameter binding. Any authenticated user can use blind, time-based queries to infer and extract data accessible to the ProcessMaker database account. This issue is fixed in version 2026.14.3.	6.5	More Details
CVE-2026-109170	LogicalDOC Community Edition through 9.3 contains an HQL injection vulnerability in DocumentsDataServlet that allows authenticated users to manipulate queries via the unvalidated indexed parameter. Attackers with read access to any folder can inject boolean HQL expressions to bypass folder scope and read-permission checks, listing restricted document metadata and extracting database contents.	6.5	More Details

CVE-2026-103070	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShortPixel ShortPixel Image Optimizer shortpixel-image-optimiser allows Stored XSS.This issue affects ShortPixel Image Optimizer: from n/a through 6.5.6.	6.5	More Details
CVE-2026-107336	Malcolm's front nginx reverse proxy defines a "Dashboards → Arkime shortcut" location using a case-insensitive regex matcher but a case-sensitive rewrite. A request whose path segment is not exact-lowercase (for example /IDDASH2ARK/...) enters the location (the matcher fires) but evades the rewrite (no redirect is issued), so nginx falls through to the location's proxy_pass to the Arkime backend. That location is the one proxied location in the shipped config that does not include the per-location authentication file, so the request reaches Arkime unauthenticated. The same location also forwards a client-supplied X-Forwarded-User header un-overwritten, and Arkime is configured to trust X-Forwarded-User as the authenticated username — so an unauthenticated network caller can reach the Arkime backend while supplying a forged, auto-provisioned identity.	6.5	More Details
CVE-2026-14273	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a local attacker to obtain sensitive information due to improper authorization.	6.5	More Details
CVE-2026-14508	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service and obtain sensitive information due to a use-after-free.	6.5	More Details
CVE-2026-14988	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 is vulnerable to buffer overflow.	6.5	More Details
CVE-2026-46438	wger is a free, open-source workout and fitness manager. Prior to version 2.6, an authenticated attacker can inject arbitrary workout log entries into any other user's `SlotEntry` by supplying the victim's `slot_entry` ID in a `POST /api/v2/workoutlog/` request. The `slot_entry` foreign key is not included in the ownership verification performed by `WorkoutLogViewSet.get_owner_objects()`, so the server accepts and persists the cross-user reference without error. Because `SlotEntry.get_config_data()` retrieves associated logs via `self.workoutlog_set.all()` with no user filter, the attacker's injected data is silently folded into the victim's progressive-overload calculations, corrupting their auto-generated weight and repetition targets. Version 2.6 contains a patch.	6.5	More Details
CVE-2026-107287	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.77.0 until 1.107.7 and 2.52.0, the local web_fetch_tool and the WebFetch local fallback can consume excessive CPU and memory during HTML-to-Markdown conversion of attacker-controlled HTML containing deeply nested block elements. Conversion repeatedly reprocesses accumulated text and can greatly expand intermediate output before the returned-content limit is applied, allowing a model-directed fetch to delay other work in the process. Provider-native web fetching is not affected. This issue is fixed in versions 1.107.7 and 2.52.0.	6.5	More Details
CVE-2026-107290	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.77.0 until 1.107.6 and 2.44.0, the local web_fetch_tool and the WebFetch local fallback process server-controlled responses with quadratic title extraction, whitespace normalization, and ordered-list numbering. An attacker-controlled page of modest size can therefore block the event loop for an extended period, stalling other agent runs and requests, while unsupported codecs or excessive HTML or JSON nesting can abort an individual run. This issue is fixed in versions 1.107.6 and 2.44.0.	6.5	More Details
CVE-2026-107294	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.77.0 until 1.107.2 and 2.24.0, web_fetch_tool, the WebFetch local fallback, and remote FileUrl media downloads buffer the complete HTTP response body before enforcing content-size controls. An attacker-influenced URL can stream an arbitrarily large response that exhausts process memory and crashes the worker; affected media types include ImageUrl, DocumentUrl, VideoUrl, and AudioUrl. SSRF protections remain effective, and the impact is limited to availability. This issue is fixed in versions 1.107.2 and 2.24.0.	6.5	More Details
CVE-2026-107301	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, constructing msgpack5 with an empty or partial options object disables the default protoAction: 'error' protection. A decoded map containing a __proto__ key can then replace the decoded object's prototype, potentially changing inherited properties or downstream behavior, although Object.prototype is not modified globally. This issue is fixed in version 6.1.0.	6.5	More Details
CVE-2026-105078	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Store Locator WP Store Locator wp-store-locator allows Stored XSS.This issue affects WP Store Locator: from n/a through 3.0.3.	6.5	More Details
CVE-2026-50055	A policy-enforcement flaw in Zimbra Collaboration Suite allows an authenticated user to bypass disabled mail forwarding by using a Sieve notify action to send copies of email content and headers to an arbitrary address.	6.5	More Details
	Path traversal of 'trusted_jar_paths' in Impala 4.5.2 allows an attacker-controlled JAR to be loaded via a		

CVE-2026-90466	relative path where the prefix matches a path specified in 'trusted_jar_paths'. The startup flag 'trusted_jar_paths' references URIs for loading files from local or remote filesystems. Path traversal can't override the schema, but can result in loading a JAR that has been uploaded to a different location in that filesystem via Impala DDLs such as CREATE DATA SOURCE and CREATE TABLE. Path traversal can only be used if a trusted path exists, so this attack requires 'trusted_jar_paths' have a non-empty value configured by the Impala admin. Users are recommended to upgrade to version 4.5.3, which fixes this issue.	6.5	More Details
CVE-2026-107335	Malcolm's upload-processing pipeline (scripts/safe-extract.py) enforces entry-count, nesting-depth, and total-uncompressed-byte limits when extracting container archives (zip/tar/rar/7z via libarchive), but those limits are not applied when the uploaded file is a single-stream compressed format (.gz, .bz2, .xz, .lzma, .lz) that isn't a .tar.*-style archive. Any authenticated user permitted to upload PCAP/log files can upload a small, highly compressible file (e.g. a gzip bomb) that decompresses to an effectively unbounded size on disk, exhausting the shared Docker volume used by OpenSearch, Logstash, Arkime, and Zeek, and disrupting the platform for all users.	6.5	More Details
CVE-2026-107379	savg-sanitizer is a PHP SVG/XML sanitizer. Prior to 1.0.0, svg-sanitizer allows a crafted SVG DTD with a #FIXED attribute default to make cleanAttributesOnWhitelist() perform a double DOMELEMENT::removeAttribute() call on the same attribute name in src/Sanitizer.php. The first removal deletes the explicit attribute, while the DTD default rematerializes the value before the href safety path performs the second removal, which can corrupt libxml state and terminate the PHP worker. An attacker who can submit SVG content to a sanitization endpoint can repeatedly interrupt workers and degrade or exhaust application availability. This issue is fixed in version 1.0.0.	6.5	More Details
CVE-2026-12859	Missing Authorization vulnerability in Caz Informatics Services Trade Inc. Advancity ALMS Cloud allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Advancity ALMS Cloud: through 2026-10-08. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2026-107695	FFmpeg before 8.1.3 contains an infinite loop vulnerability in the HLS demuxer that allows remote attackers to cause denial of service because parse_playlist() accepts Master Playlist tags inside Media Playlists. Attackers can trick victims into opening a crafted self-referencing playlist that endlessly adds variants in hls_read_header(), causing unbounded CPU and I/O consumption.	6.5	More Details
CVE-2026-107696	FFmpeg through 9.0.2 contains an infinite loop vulnerability in ff_rtsp_connect() in libavformat/rtsp.c that follows RTSP 3xx redirects without any redirect limit. Attackers controlling an RTSP server can answer every request with a 302 redirect to itself or another server, causing endless reconnects that saturate a CPU core.	6.5	More Details
CVE-2026-62179	PraisonAI is a multi-agent teams system. In `praisonai-platform` prior to version 0.1.9, issue dependency deletion can be authorized against the wrong side of a dependency edge. A workspace member cannot delete a dependency through the owner-created issue endpoint, but can delete the same dependency through a member-owned related issue endpoint because the route accepts either endpoint and checks delete permission only against the caller-selected URL issue. Version 0.1.9 patches the issue.	6.5	More Details
CVE-2026-107121	A flaw was found in the SMTP email configuration handling of the keycloak-services component. When the STARTTLS option is enabled, Keycloak fails to strictly enforce an encrypted connection, allowing it to fall back to unencrypted communication if the encryption request is tampered with. An attacker who can intercept network traffic can exploit this to capture sensitive email credentials and message content in plain text.	6.5	More Details
CVE-2026-96530	The Optimole WordPress plugin before 4.2.15 does not perform a capability check before exposing its stored image-optimization account data in a dashboard widget, allowing any authenticated user, including Subscribers, to read the site's third-party service credentials.	6.5	More Details
CVE-2026-106429	An integer underflow in the KMS endpoint-parsing logic of MongoDB libmongocrypt can cause an allocation failure that terminates the application process. This can occur when an authenticated user modifies a key document in the key vault collection, or when an application accepts a KMS endpoint containing a colon after its path or query during key creation. The issue does not access memory outside its allocated bounds.	6.5	More Details
CVE-2026-87668	A stack-based buffer overflow vulnerability exists in the diagnostic execution utility of Brocade Fabric OS versions before 10.0.1. When processing command arguments for diagnostic operations, the utility tokenizes user-supplied input into an internal argument array without enforcing boundary checks on the maximum array capacity. An authenticated user with administrative access can exploit this vulnerability by supplying a crafted diagnostic command string containing an excessive number of tokenized arguments. This leads to a memory overwrite resulting in a denial of service (process crash).	6.5	More Details
CVE-2017-20283	NXP MQX Classic before 5.0 contains an out-of-bounds write vulnerability in the RTCS UDP recvfrom() implementation. Improper enforcement of the application-supplied receive buffer length may allow a crafted UDP packet to overflow the destination buffer, resulting in memory corruption, or denial of service.	6.5	More Details
CVE-2026-103378	The Geliver Akıllı Kargo Pazaryeri WordPress plugin before 3.1.1 does not prevent unauthenticated access to a log file it stores within its own web-accessible directory, into which it writes the site's carrier integration key while processing requests from unauthenticated users, allowing attackers to retrieve the key and use it to modify WooCommerce order statuses. The same log file also exposes customer information from orders the shop has processed.	6.5	More Details

CVE-2026-103869	A flaw was found in pulp-ansible's bearer-token refresh for collection remotes. The access token is kept in one module-level variable and reused for every token download in that worker. A user who can sync an Ansible remote that uses token refresh, and can point that remote at a server they control, receives an access token obtained for a different remote, and can reuse it at the service that issued it. Content stored in Pulp is not changed, and the service is not stopped.	6.5	More Details
CVE-2026-103868	A flaw was found in pulp-container when it authenticates to an upstream registry. Basic and bearer credentials from one remote are reused for later downloads in the same worker. A user who can sync a container remote, and can point that remote at a server they control, receives the username, password, or bearer token stored for a different remote, and can reuse that credential at the upstream registry. Content stored in Pulp is not changed, and the service is not stopped.	6.5	More Details
CVE-2026-107705	Poppler 0.42.0 through 26.10.0 contains a stack-based buffer overflow in Decrypt::revision6Hash() that allows attackers controlling the password to overwrite stack memory when opening AESV3/R6 encrypted PDFs. Attackers can supply a password longer than 127 bytes through applications using the libpoppler, libpoppler-glib or C++ API to overflow the K1 and E buffers, crashing the process or corrupting memory.	6.5	More Details
CVE-2026-13257	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow an authenticated user to forge signature requests due to improper verification of data authenticity.	6.5	More Details
CVE-2026-94245	The Wallet System for WooCommerce WordPress plugin before 2.8.0 does not verify that the user submitting a wallet transfer owns the wallet being debited, allowing any authenticated user, including one with only the Subscriber role, to move an arbitrary user's wallet balance, including an administrator's, into an account they control.	6.5	More Details
CVE-2026-84274	IBM Guardium Data Protection 12.2.2 is affected by a sensitive information exposure vulnerability. During SECRET and API_KEY rotation processing, sensitive credential material is logged at INFO level by the edge-controller/edge-manager components. An authenticated attacker with access to the relevant application or container logs could obtain these credentials and use them to impersonate services or gain unauthorized access to the Guardium control plane.	6.5	More Details
CVE-2026-62127	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MediaRon LLC WP Plugin Info Card wp-plugin-info-card allows Stored XSS.This issue affects WP Plugin Info Card: from n/a through 6.3.5.	6.5	More Details
CVE-2026-105079	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StylemixThemes MasterStudy LMS masterstudy-lms-learning-management-system allows Stored XSS.This issue affects MasterStudy LMS: from n/a through 3.7.52.	6.5	More Details
CVE-2026-107159	MiniUPnPd through 2.3.11 built with --strict contains a divide-by-zero vulnerability in ProcessSSDPData() that allows unauthenticated local network attackers to crash the daemon. Attackers can send a single multicast M-SEARCH datagram with MX: 0 and a known ST to port 1900, triggering SIGFPE and denying UPnP IGD service.	6.5	More Details
CVE-2026-105886	Missing Authorization vulnerability in BdThemes Ultimate Post Kit ultimate-post-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Post Kit: from n/a through 4.5.5.	6.5	More Details
CVE-2026-105887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robosoft Robo Gallery robo-gallery allows Stored XSS.This issue affects Robo Gallery: from n/a through 5.1.6.	6.5	More Details
CVE-2026-105138	Obot 0.12.0 before 0.26.2 contains an insufficiently protected credentials vulnerability that allows authenticated users to read static secrets set on MCP catalog entries by admins or power users. Basic users granted an entry by access control rules can request GET /api/all-mcps/entries/{entry_id} to obtain plaintext API keys or tokens and abuse them against backend services.	6.5	More Details
CVE-2026-105890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP Gutenberg Blocks by Kadence Blocks kadence-blocks allows Stored XSS.This issue affects Gutenberg Blocks by Kadence Blocks: from n/a through 3.7.12.	6.5	More Details
CVE-2026-107583	Inefficient algorithmic complexity in the webmail's message view of the REST API in Progressive Robot hMailServer 6.3.2 through 6.3.5 allows a remote unauthenticated attacker to make the webmail, the administration console and the REST API unavailable by sending a message. The route that renders a received message's HTML replaced each reference to an embedded image in place, with work that grew with the square of the number of references, and wrote the image out for every reference while counting it against its size limit only once. A message whose HTML refers to one small embedded image a very large number of times, opened in the webmail by its recipient, therefore keeps one of the listener's four worker threads busy for minutes and makes it build a document of gigabytes, so that a few such messages leave the HTTP listener unable to answer anybody.	6.5	More Details

CVE-2026-107582	Inefficient algorithmic complexity in the REST API (6.3.3 through 6.3.5) and the IMAP PREVIEW response (6.2.22 through 6.3.5) of Progressive Robot hMailServer allows a remote unauthenticated attacker to make the webmail, the administration console and the REST API unavailable by sending a message. To show a snippet of each message in a folder's message list, the server decoded the character entity references of a message that has an HTML part and no text part with a string replacement whose work grew with the square of their number. A received HTML-only message holding a very large number of entity references therefore keeps one of the listener's four worker threads busy for minutes or longer each time the recipient's webmail lists the folder, without the message being opened, so that a few such listings leave the HTTP listener unable to answer anybody. The IMAP PREVIEW response read such text the same way, holding an IMAP thread for each client that asks for the preview of such a message. The flaw is in the server's shared string class, whose replace and remove both ran in quadratic time.	6.5	More Details
CVE-2026-106603	Authorization Bypass Through User-Controlled Key vulnerability in Groundhogg HollerBox holler-box allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HollerBox: from n/a through 2.3.14.	6.5	More Details
CVE-2026-107581	Progressive Robot hMailServer 6.0.0 through 6.3.5 processes several IMAP commands from a signed-in account in time quadratic in the command's length or in the number of elements it names, and can be made to hold memory out of proportion to a command. The FETCH data-item parser normalised a BODY[] section with a case-insensitive string replacement that copied the whole item per occurrence and split the item list by repeatedly copying the remainder of the command; the server's case-insensitive search compared a needle afresh at every position, so a long SEARCH TEXT key over a message cost the product of the two lengths; SEARCH message sets and the saved-result marker (\$), SORT criteria, HEADER.FIELDS name lists and UID ranges were each read once per message rather than once per command; and a FETCH naming a message's sections very many times read and held every section in memory before sending any. An IMAP command may continue past one line through non-synchronizing literals, so one command can reach about eleven megabytes. The IMAP worker threads are a small pool shared with SMTP and POP3, so a signed-in user sending such commands can make the IMAP, SMTP and POP3 services stop responding (CWE-407) and can consume excessive memory (CWE-400).	6.5	More Details
CVE-2026-107580	Inefficient algorithmic complexity in the decoding of message header fields in Progressive Robot hMailServer 6.0.0 through 6.3.5 allows a remote unauthenticated attacker to make the IMAP, SMTP and POP3 services, or the webmail, unavailable by sending a message. The server unfolded a decoded header value by finding each line break from the end of the value and removing it, moving the rest of the value each time, so its work grew with the square of the number of line breaks, and an RFC 2047 encoded word may decode to any number of them. A received message whose Subject or other header field holds such a value keeps a worker thread busy for minutes or longer each time the value is read: when the recipient's IMAP client searches, sorts or threads the folder by a header, when the webmail lists the folder, and, where configured, when a rule tests a header, a spam tag is added to the Subject or an abuse report is read during delivery. The IMAP worker threads are shared with SMTP and POP3, so a few such messages stop those services responding. The server's reading of a message header from its file also searched everything read so far after each 4,000 bytes, costing seconds for a header of tens of megabytes.	6.5	More Details
CVE-2026-107572	Inefficient complexity in the Sieve filter evaluation of Progressive Robot hMailServer 6.2.24 through 6.3.5 allows an authenticated account holder to make the mail services unavailable with their own filter. A ':matches' pattern was matched by a backtracking descent whose time grew with the matched value's length raised to the number of wildcards, so a pattern such as '*a*a*a*b' over 800 characters took 44 seconds; and 'deleteheader' erased the fields it removed one at a time, so removing many fields of one name over a message's header cost $O(N^2)$ (80,000 fields took 18.8 seconds). Sieve filters run on the small, shared delivery thread pool, so an account holder whose active script does this, fed a few messages they can send themselves, empties the pool and stops delivery for the whole server. The script is the account holder's own and cannot be set for another user.	6.5	More Details
CVE-2026-41958	A path traversal vulnerability exists in the unzip_http RemoteZipFile extract functionality of VisiData (version(s): dev (commit 38b21f78)). A specially crafted .zip file can lead to arbitrary file write. An attacker can provide a crafted URL to trigger this vulnerability.	6.5	More Details
CVE-2026-107636	pH7Builder (pH7 Social Dating CMS) before 18.5.1 contains a payment validation vulnerability that allows registered low-privileged members to obtain any membership tier by supplying client-controlled plan and amount fields. Attackers can set item_number, cart_order_id, or the PayPal custom field while paying a token amount, or submit uncompleted PayPal IPN payments, to gain the most expensive membership and its paid features.	6.5	More Details
CVE-2026-93509	The Wallet System for WooCommerce WordPress plugin before 2.8.0 does not validate that a wallet transfer amount is positive, and computes the sender's new balance from a stale snapshot taken before crediting the recipient, allowing an authenticated attacker with Subscriber-level access to mint wallet funds for themselves or drain a specific victim's balance into their own account.	6.5	More Details
CVE-2026-27420	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Katie Seaborn Zotpress zotpress allows Stored XSS.This issue affects Zotpress: from n/a through 7.4.4.	6.5	More Details

CVE-2026-103011	Heap-based buffer overflow in the legacy Blowfish encryption routine (BlowFishEncryptor::Encode, called by EncryptToString) in Progressive Robot hMailServer 6.0.0 through 6.3.5 allows an authenticated mailbox user to cause a denial of service (service crash), and possibly other unspecified impact. In 6.3.4 and 6.3.5, where the self-service REST API is enabled (it is off by default), the user does this remotely by adding a fetch account whose password is 129 to 247 characters long and not a multiple of 8, and then requesting their personal data export (GET /api/v1/me/export.zip), which encrypts that password with the legacy scheme. The same flaw is reachable on Windows by any local interactive user with no hMailServer credentials, through the COM method Utilities.BlowfishEncrypt, which checked no authentication. It is also reachable by every stored-secret write when ProtectStoredSecretsWithDPAPI is set to 0. For such a length, the routine's padding loop writes up to 7 zero bytes 2 to 232 bytes past the end of its 255-byte heap buffer. The ciphertext it returns is still correct.	6.5	More Details
CVE-2026-71896	An authorization vulnerability in Apache DolphinScheduler allows authenticated users to retrieve other users' account information through the /dolphinscheduler/users/list-all endpoint without the required permissions. The endpoint fails to enforce the necessary authorization checks before returning user account information. As a result, an authenticated user can access account information they are not authorized to view. Successful exploitation may expose sensitive user information and facilitate account enumeration. This issue affects Apache DolphinScheduler: before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	6.5	More Details
CVE-2026-66082	An authorization bypass vulnerability in Apache DolphinScheduler allows authenticated users to perform unauthorized operations on workflow schedules, workflow definitions, and task instances in other projects. The affected endpoints check permissions against the supplied projectCode but fail to verify that the target resource belongs to that project. An authenticated user with the required permissions in one project can supply that project's code together with a resource identifier from another project, bypassing the target project's access restrictions. The affected endpoints include: * POST /projects/{projectCode}/schedules/{id}/online and /offline: Activate or deactivate workflow schedules in another project. * POST /projects/{projectCode}/workflow-definition/{code}/release: Change the ONLINE/OFFLINE state of workflow definitions in another project. Successful exploitation allows users to alter workflow availability and interfere with task execution in projects they are not authorized to access. This issue affects Apache DolphinScheduler: before 3.4.3. Users are recommended to upgrade to version 3.4.3, which fixes the issue.	6.5	More Details
CVE-2026-97294	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant media-library-assistant allows Stored XSS.This issue affects Media Library Assistant: from n/a through 3.41.	6.5	More Details
CVE-2026-105884	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Media Rocket Lazy Load rocket-lazy-load allows Stored XSS.This issue affects Rocket Lazy Load: from n/a through 2.4.0.	6.5	More Details
CVE-2026-105875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Prime Slider – Addons For Elementor bdthemes-prime-slider-lite allows Stored XSS.This issue affects Prime Slider – Addons For Elementor: from n/a through 4.6.2.	6.5	More Details
CVE-2026-105873	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons bdthemes-element-pack-lite allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 8.8.6.	6.5	More Details
CVE-2026-105871	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons bdthemes-element-pack-lite allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 8.8.6.	6.5	More Details
CVE-2026-104393	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weDevs Happy Addons for Elementor happy-elementor-addons allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.50.0.	6.5	More Details
CVE-2026-104391	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpressTech Quiz And Survey Master quiz-master-next allows Stored XSS.This issue affects Quiz And Survey Master: from n/a through 11.2.7.	6.5	More Details
CVE-2026-76274	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the read_o11y_content capability could redirect an outbound request from Splunk App for Splunk Observability Cloud through the Representational State Transfer (REST) API to an attacker-controlled host and disclose the configured Observability Cloud Application Programming Interface (API) token. The vulnerability is possible because Splunk App for Splunk Observability Cloud does not fully validate the destination of an outbound request. For more information see Authentication tokens (https://help.splunk.com/en/splunk-observability-cloud/administer/authentication-and-security/authentication-tokens) in the Splunk documentation. Splunk Enterprise versions 9.4.x are not affected.	6.5	More Details
CVE-2026-	An authorization bypass in the EWS FindItem handler of Zimbra Collaboration Suite 10.1.0 through 10.1.19 allows an authenticated user with EWS enabled to read complete mailbox items, including raw MIME and	6.5	More

10631	attachments, from arbitrary local accounts without a share or delegation grant.		Details
CVE-2026-19878	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to bypass additional authentication workflow steps.	6.5	More Details
CVE-2026-107225	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.8.0 to 2.11.0, GetStyle's fill, border, and font extraction predicates check only upper bounds for attacker-controlled style-table indices. File.GetStyle relies on extractStyleCondFuncs predicates that allow negative FillID, BorderID, and FontID values to reach slice indexing. When a crafted styles.xml supplies a negative fillId, borderId, or fontId and the application reads the style, a negative identifier passes the upper-bound-only predicate and becomes a negative slice index, allowing an attacker to panic while reading cell styling. No fixed version is available as of this review.	6.5	More Details
CVE-2026-76265	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, and Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72, a user who does not hold the "admin" or "power" Splunk roles could access privileged Splunk Secure Gateway functionality. With this access, the user could cause Splunk Secure Gateway to sign attacker-controlled payloads. The vulnerability is possible because multiple Splunk Secure Gateway Representational State Transfer (REST) API endpoints do not enforce authorization requirements before processing requests.	6.5	More Details
CVE-2026-1403	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.7 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that when importing CSV files could have allowed an authenticated user to cause denial of service to Sidekiq workers due to improper validation of CSV file structure.	6.5	More Details
CVE-2026-107778	MIT Kerberos 5 (krb5) through 1.22.2 contains a NULL pointer dereference in make_cred_list() in rd_cred.c that allows authenticated Kerberos clients to crash services by sending mismatched KRB-CRED arrays. Attackers can send forwarded credentials with more tickets than ticket_info entries through gss_accept_sec_context() to crash GSS-API acceptor services, causing denial of service.	6.5	More Details
CVE-2026-76488	A vulnerability in the export policies functionality of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to access sensitive files on an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient access control to file system resources. An attacker could exploit this vulnerability by submitting crafted values in specific UI fields. A successful exploit could allow the attacker to access sensitive files from the underlying file system of an affected device, including key materials that could be used to elevate privileges to root on the affected APIC and on managed switches.	6.5	More Details
CVE-2026-107220	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.7.1 to 2.11.0, mergeCellsParser leaves the cached rectangle empty for an empty mergeCell ref and then passes that empty slice to cellInRange without a length check. GetCellValue reaches mergeCellsParser, which passes an empty rectangle derived from the mergeCell ref attribute into cellInRange. When a crafted worksheet contains an empty mergeCell ref and a non-streaming cell API reads the worksheet, cellInRange indexes four positions in an empty slice, allowing an attacker to panic on the first affected cell operation. No fixed version is available as of this review.	6.5	More Details
CVE-2026-76269	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the "admin" or "power" Splunk roles could use a user-controlled job identifier to access substantially all search job information from jobs that belong to other users, including search query text, job metadata, results, and preview results, through an Application Programming Interface (API) implemented as a Representational State Transfer (REST) API. The vulnerability is possible because the REST API does not fully validate job ownership before returning search job information.	6.5	More Details
CVE-2026-107221	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.0.0 to 2.11.0, checkRow sizes its target cell slice from the last cell in XML document order and then re-scatters every cell by its explicit column reference. GetCellValue reaches workSheetReader and checkRow, where targetList is too short for an earlier out-of-order cell. When a crafted row places a higher-column cell before a lower-column final cell and a non-streaming worksheet API reads the sheet, the earlier cell's column index exceeds the slice length derived from the final cell, allowing an attacker to cause an unrecovered panic and terminate the process. No fixed version is available as of this review.	6.5	More Details
CVE-2026-107222	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.7.0 to 2.11.0, conditional-format extraction indexes required child slices or dereferences an optional colorScale child without validating malformed rule structure. GetConditionalFormats reaches extractCondFmtCells and also indexes ColorScale.Cfvo, DataBar.Cfvo, and DataBar.Color without complete structural checks. When a crafted worksheet supplies a cells, dataBar, or colorScale rule missing expected children and the application calls GetConditionalFormats, missing formula, color, value-object, or colorScale data reaches an out-of-range index or nil dereference, allowing an attacker to panic and terminate an unprotected process. No fixed version is available as of this review.	6.5	More Details
	A vulnerability in the web-based management API for Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to execute arbitrary commands as the root user. To exploit		

CVE-2026-20321	this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient input validation of user-controlled command arguments. An attacker could exploit this vulnerability by authenticating using the API and sending crafted input. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of an affected device with root-level privileges.	6.5	More Details
CVE-2026-107224	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.1.0 to 2.11.0, a Zip64 uncompressed size with the high bit set is converted from uint64 to a negative int64 before signed size-limit checks and allocation. ReadZipReader obtains UncompressedSize64 through FileInfo.Size and passes the wrapped negative value to readFile. When a crafted Zip64 entry declares an uncompressed size from 2^{63} through $2^{64}-1$ and the workbook is opened, the negative size bypasses unzip limits and reaches make as a negative capacity, allowing an attacker to panic during workbook opening. No fixed version is available as of this review.	6.5	More Details
CVE-2026-97671	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to a path traversal vulnerability.	6.5	More Details
CVE-2026-93448	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	6.5	More Details
CVE-2026-101329	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to obtain sensitive information due to improper access control.	6.5	More Details
CVE-2026-78399	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow an authenticated user to cause a denial of service using a specially crafted HTTP query due to improper allocation of system resources	6.5	More Details
CVE-2026-107353	traverse (npm) versions 0.3.6 through 0.3.9, 0.4.0 through 0.4.6, 0.5.0 through 0.5.2, and 0.6.0 through 0.6.11 allow prototype pollution through set(). When the path passed to set() crosses a primitive value, the next path segment is resolved on that primitive's built-in prototype, so an application that passes an untrusted path to set() lets an attacker add or overwrite properties of String.prototype, Number.prototype, or Boolean.prototype using plain JSON data, for example traverse({ name: 'bob' }).set(['name', '__proto__', 'polluted'], 'yes'). Object.prototype was reachable only with a non-data path segment, such as an object whose toString returns a different value on each call, or through a Proxy that accepts an assignment without storing it. This is fixed in 0.3.10, 0.4.7, 0.5.3, and 0.6.12.	6.5	More Details
CVE-2026-104628	Satel Netco Design versions prior to v2.1.7 contains an inefficient regular expression complexity vulnerability. An authenticated user with Viewer privileges could submit crafted search input that causes excessive processing, potentially degrading the availability of the application.	6.5	More Details
CVE-2026-76270	In Splunk Enterprise versions below 10.4.3, a user that holds a role with the list_spl2_modules capability could use SQL injection in SPL2 module filtering to access all relevant data available through the affected Representational State Transfer (REST) API, including private SPL2 module definitions belonging to other users. The vulnerability is possible because Splunk Enterprise and Splunk Cloud Platform do not parameterize user-supplied values before using them in database queries for SPL2 module filtering. For more information see Manage SPL2 modules (https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/multiple-searches-in-an-spl2-module/manage-spl2-modules) and Module permissions (https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/modules-statements-and-views/module-permissions) in the Splunk documentation. Splunk Enterprise versions 10.2.x, 10.0.x, and 9.4.x are not affected.	6.5	More Details
CVE-2026-76271	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a low-privileged user that does not hold the "admin" or "power" Splunk roles could cause a denial of service against a Representational State Transfer (REST) API endpoint in the Discover Splunk Observability Cloud app. The vulnerability is possible because the app uses an inefficient regular expression to validate input submitted through the endpoint. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access), Splunk Observability Cloud previews (https://help.splunk.com/en/splunk-enterprise/search/search-manual/10.4/observability/splunk-observability-cloud-previews), and restmap.conf (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/configuration-file-reference/10.4.0-configuration-file-reference/restmap.conf) in the Splunk documentation. Splunk Enterprise versions 9.4.x are not affected.	6.5	More Details
CVE-2026-6243	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via kses bypass / mutation XSS in all versions up to, and including, 3.28.36. This is due to the 'get_dynamic_values' function performing text-level find-and-replace operations on post content without HTML-aware parsing. 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-2026-97340	The Avada Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to Stored Cross-Site Scripting via the user profile 'Author Page' social link contact-method fields (author_facebook, author_twitter, author_linkedin, author_dribble, author_whatsapp, author_email) in versions up to, and including, 7.16.1. Avada registers these fields through the user_contactmethods filter and, on the author archive, emits them inside an anchor href using only esc_attr() in Fusion_Social_Icon::get_markup(), which escapes HTML metacharacters but does not reject dangerous URL schemes such as javascript:. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses their author page and clicks the injected social icon (a click is required, and the site must have 'Open Social Icons in a New Window' set to Off so the browser doesn't block the javascript: URL from opening in a new tab).	6.4	More Details
CVE-2026-102402	The Team – Team Members Showcase Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ttp_filter_taxonomy (meta of the attacker-chosen post)' parameter in all versions up to, and including, 6.0.2 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-2026-103427	The Simple Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'country' parameter in all versions up to, and including, 4.8.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Unauthenticated attackers may also exploit this vulnerability when the plugin's Enable Free Membership feature is turned on, as it permits anonymous front-end registration and profile submission.	6.4	More Details
CVE-2026-97643	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `givewp_campaign_grid` shortcode in versions up to, and including, 4.17.0 This is due to insufficient input sanitization and output escaping on user supplied shortcode attributes (`filter_by`, `layout`, `sort_by`, `order_by`) in the CampaignGridShortcode::parseAttributes() function combined with the render template emitting `json_encode(\$attributes)` inside a single-quoted HTML attribute without esc_attr() — json_encode() does not escape single quotes by default, so a `` in an attribute value breaks out of the enclosing attribute. 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-2026-108593	9router 0.4.1 through 0.5.99 contains a configuration injection vulnerability in the POST /api/cli-tools/hermes-settings endpoint that allows authenticated dashboard users to inject arbitrary keys into the Hermes Agent config.yaml file. Attackers can submit a baseUrl containing double quotes and newlines to add hooks_auto_accept and a hooks.post_llm_call shell command, which Hermes Agent executes without approval after an LLM call.	6.4	More Details
CVE-2026-107822	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, MariaDB's ACL cache could generate the same database-privilege cache key for role and localhost user names that matched because both used an empty IP component. An attacker with CREATE USER could create the colliding principal and, when the original principal's database privileges were cached, exercise privileges assigned to the other account. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	6.4	More Details
CVE-2026-11888	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 is vulnerable to an information disclosure attack.	6.4	More Details
CVE-2026-96574	The User Frontend – Membership, User Registration, User Profile, User Directory & Content Restriction with Frontend Post Submission plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpuf_payment_method' parameter in all versions up to, and including, 4.3.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The bypass technique involves appending a valid gateway keyword such as 'bank' to the HTML payload, causing sanitize_text_field() to yield only the keyword for routing purposes while the full malicious raw value is stored and later rendered unescaped.	6.4	More Details
CVE-2026-106177	A kernel buffer overflow vulnerability in HP Sure Click versions prior to 4.4.33 may allow local privilege escalation or arbitrary code execution. HP has released version 4.4.33 to address this vulnerability.	6.4	More Details
CVE-2026-102774	The SureDash – Community, Courses & Member Dashboard plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via Image 'alt' Attribute in Community Post Content in all versions up to, and including, 1.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The entity-encoded payload bypasses server-side wp_kses filtering because kses permits the img/alt tag combination and does not normalize entities inside attribute values; the decode occurs client-side when GLightbox reads the .alt DOM property and assigns the result to innerHTML.	6.4	More Details

CVE-2026-103478	The Premium Packages – Sell Digital Products Securely plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'checkout[billing][phone] (and state / taxid / email)' parameter in all versions up to, and including, 7.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-94421	The Church Admin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in all versions up to, and including, 5.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4791	The PeproDev Ultimate Profile Solutions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `logout-url` shortcode's 'button' attribute in all versions up to, and including, 8.2.36 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-2026-96563	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'stm_f_s' parameter in all versions up to, and including, 1.4.123 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The nonce required by the stm_ajax_add_a_car AJAX handler is emitted in wp_footer on every page, making it accessible to any authenticated user and removing any practical barrier to exploitation at the Subscriber level.	6.4	More Details
CVE-2026-107174	A flaw was found in source-to-image. When unpacking archive files, the application fails to properly sanitize symbolic links pointing to absolute file paths. An attacker who supplies a malicious builder image can exploit this vulnerability by embedding links pointing outside the extraction directory. This allows the attacker to bypass sandbox boundaries, potentially leading to unauthorized information disclosure or file modification on the host system.	6.4	More Details
CVE-2026-107292	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.34.0 until 2.30.0, the Agent.to_web() and clai web development chat server does not validate the Host header, allowing a website visited by a developer to use DNS rebinding to reach a loopback-hosted agent as a same-origin service. The hostile page can read the served UI and submit chat requests that execute agent tools with the local process's privileges and credentials, causing data disclosure or unwanted side effects. Binding to localhost, Origin checks, and CSRF tokens do not prevent the same-origin DNS rebinding path. This issue is fixed in versions 1.107.5 and 2.30.0.	6.4	More Details
CVE-2026-97396	The Email Marketing for WordPress and WooCommerce – Retainful plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data' parameter in all versions up to, and including, 1.0.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-104762	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Block Font Family Attribute in all versions up to, and including, 3.7.12 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. This encoding bypass is only triggered when the "Load Google Fonts Locally" site option (kadence_blocks_font_settings['load_fonts_local']) is enabled, which is not the default configuration.	6.4	More Details
CVE-2026-96743	The Table Field Add-on for ACF and SCF plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Table Field Value in all versions up to, and including, 1.4.1-RC2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-9696	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'not_found' parameter in all versions up to, and including, 3.3.58 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-2026-97630	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Unquoted popup Shortcode Attribute in all versions up to, and including, 7.5.54.7212 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires the profile_videos_enable_bio option to be enabled, as script execution occurs on the author bio/archive page where the profile-video shortcode is rendered.	6.4	More Details
CVE-	The Data Tables Generator by Supsysytic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Table Cell 'data' Value via updateRows Action in all versions up to, and including, 1.15.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-		More

2026-96648	level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable by Subscriber-level users when an administrator has added their role to the plugin's 'access_roles' setting, which is a documented and explicitly supported plugin feature that grants lower-privileged users access to the dtgs_nonce required to reach the vulnerable updateRows action handler.	6.4	Details
CVE-2026-14379	The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_id' parameter in all versions up to, and including, 7.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-104993	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email (Contact Email custom field htmlvar_name)' parameter in all versions up to, and including, 2.8.188 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires that an administrator has added and configured the Contact Email custom field to render on the public single-listing output page, and that the administrator subsequently approves the attacker's submitted listing.	6.4	More Details
CVE-2026-14877	The Data Tables Generator by Supsysitic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the id attribute in all versions up to, and including, 1.12.03 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-2026-104735	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Feedzy Loop Block Feed URL / RSS <title> in all versions up to, and including, 5.2.10 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. The payload is not neutralized at save time because post_content stores only a benign block reference to an external feed URL; the malicious HTML is injected at render time from the attacker-controlled RSS feed title, bypassing any save-time wpkses filtering.	6.4	More Details
CVE-2026-102401	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'regurl' parameter in all versions up to, and including, 3.3.71 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. The injected payload only fires for logged-out site visitors, as the vulnerable login-form.php template branch is gated on !is_user_logged_in(); authenticated users viewing the same page are served a different template and are not affected.	6.4	More Details
CVE-2026-14882	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'brizy-compiled-sections' parameter in all versions up to, and including, 2.8.18 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-2026-16776	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 5.14.2 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. WordPress's save-time wpkses_post does not neutralize the payload because the attack is delivered via shortcode attributes rather than raw HTML in post content, allowing the unescaped values to survive to render time.	6.4	More Details
CVE-2026-93883	The Advanced Classifieds & Directory Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'phone' parameter in all versions up to, and including, 3.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is only exploitable on sites where the 'Force Bootstrap' miscellaneous setting (acadp_misc_settings['force_bootstrap']) is enabled and the 'ACADP Listing Address' widget is placed on a sidebar displayed on single listing pages; both conditions are non-default.	6.4	More Details
CVE-2026-17025	The Graphene theme for WordPress is vulnerable to Stored Cross-Site Scripting via 'Current location' and 'Author profile image URL' Profile Fields in all versions up to, and including, 2.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-	The Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embeddoc' shortcode in all versions up to, and including, 2.7.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with	6.4	More

18558	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		Details
CVE-2026-78068	The Table Field Add-on for ACF and SCF plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Table Cell Content in all versions up to, and including, 1.3.35 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-2026-91862	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data-image-points' parameter in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-107816	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the qc_info plugin could be confused by a query containing embedded null bytes. Reading information_schema.query_cache_info after such a query was cached could access data beyond the end of a heap-allocated buffer, potentially disclosing adjacent memory or crashing the server. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	6.4	More Details
CVE-2026-103520	The HivePress – Business Directory, Listings & Classified Ads Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom text attribute (user-defined field name)' parameter in all versions up to, and including, 1.7.31 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when an administrator has configured a Text attribute whose display format places the %value% token inside an HTML attribute (e.g., title="%value%"), which is a documented HivePress pattern.	6.4	More Details
CVE-2026-108794	A security vulnerability has been detected in ZKTeco BioTime 9.5.6 Build 20260130.3206. Affected by this vulnerability is an unknown functionality of the file /base/api/v1.0/systemSettings/db_migrate_setting/ of the component Database Migration Functionality. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108717	Combodo iTop 3.1.0 through 3.3.0 contains a missing authorization vulnerability in LinkSetController.php that allows authenticated console users to bypass profile grants by supplying arbitrary class and key parameters. Attackers can invoke the linkset delete, detach and get-remote-object routes to delete objects, clear external keys, and read object attributes without permission.	6.3	More Details
CVE-2026-107125	A flaw has been found in XnView Classic 2.52.5. Impacted is an unknown function of the component FLI File Parser. This manipulation of the argument starting_line causes heap-based buffer overflow. Remote exploitation of the attack is possible. Upgrading to version 2.52.6 is recommended to address this issue. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-108684	A vulnerability was detected in erzhongxmu Jeewms up to 3.7. This affects the function getTreeData of the file src/main/java/com/jeecg/demo/controller/JeecgFormDemoController.java of the component Autocomplete Data Handler. Performing a manipulation of the argument searchVal results in sql injection. The attack can be initiated remotely. The patch is named 6e29bd57972a499e9c8a81a2dbe94d0d5cf23af0. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2026-108119	A flaw was found in busybox. The tar applet's deferred link-creation handling for symlink and hardlink entries with unsafe-looking targets does not validate that the resolved destination remains inside the extraction directory once the deferred link is created. An attacker can craft a tar archive using a symlink target of exactly '..' combined with a deferred hardlink to create a new file outside the extraction directory, or reuse an extraction directory across two archives to replace an existing file outside it. If the archive is extracted with elevated privileges, this flaw can lead to privilege escalation or arbitrary code execution.	6.3	More Details
CVE-2026-106559	Backstage is an open framework for building developer portals. Prior to 0.3.25, the @backstage/plugin-scaffolder-backend-module-confluence-to-markdown package is affected by improper input validation in confluence to markdown scaffolder module. Insufficient input validation in the Confluence to Markdown scaffolder module could allow an attacker to influence file write operations during template execution. Exploitation requires a Backstage user to run a template that processes attacker-influenced Confluence content. This issue is fixed in version 0.3.25.	6.3	More Details
CVE-2026-106064	A heap-based buffer overflow was found in GIMP's GIF export plug-in. Exporting an image with very large width and height can cause 32-bit overflow when computing the pixel buffer size. The plug-in allocates a buffer based on the wrapped value while GEGL writes using the true image extent, rooted in integer overflow	6.3	More Details
CVE-2026-108890	A vulnerability has been found in BlackBeltTechnology pi-agent-dashboard up to 0.8.0. Affected by this issue is the function terminalManager.spawn of the file packages/server/src/browser-handlers/terminal-handler.ts of the component Terminal Handler. The manipulation of the argument cwd leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 48fd0bad5adfe76af9736599699d51a5f60019f6. It is suggested to install a patch to address this issue. The vendor was contacted early, responded in a very professional manner and quickly	6.3	More Details

	released a fixed version of the affected product.		
CVE-2026-108569	A vulnerability was identified in Furion .NET Framework up to 4.9.9.92. The impacted element is the function String.Replace of the file framework/Furion/Templates/Extensions/StringRenderExtensions.cs. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. 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-2026-108787	A vulnerability was found in houtini-ai voice-analyser-mcp up to 2.1.1. The affected element is the function fetch of the file src/utlis/crawler.ts of the component collect_corpus. Performing a manipulation of the argument sitemap_url results in server-side request forgery. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108786	A vulnerability has been found in houtini-ai seo-crawler-mcp up to 2.1.5. Impacted is the function run_seo_audit of the file src/core/CrawlOrchestrator.ts of the component Crawler. Such manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108544	A vulnerability was identified in Lippu Docx Reader Office Viewer App up to 1.4.5 on Android. This affects the function word.office.docxviewer.document.docx.reader.ViewTxt. Such manipulation of the argument _display_name leads to path traversal. The attack may be performed from remote.	6.3	More Details
CVE-2026-108575	A vulnerability has been found in BerriAI LiteLLM up to 1.94.0. This affects the function get_secret of the file secret_managers/main.py of the component Secret Resolution. The manipulation of the argument api_key leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-106066	A heap-based buffer overflow was found in GIMP's raw data export plug-in. When exporting very large images, g_malloc() sizing based on overflowing width * height * bytes-per-pixel can allocate far less memory than GEGL reads or writes during export, following integer overflow	6.3	More Details
CVE-2026-106067	A heap-based buffer overflow was found in GIMP's Hot color filter plug-in. For very large images, a pixel buffer is allocated using overflowing 32-bit width * height (and related) arithmetic while the filter's pixel access path uses the true image size, after integer overflow in the allocation size	6.3	More Details
CVE-2026-108543	A vulnerability was determined in ag2ai ag2 up to 0.13.4. Affected by this issue is the function os.path.join of the component UserProxyAgent. This manipulation of the argument filename causes path traversal. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108542	A vulnerability was found in 021is elvix-sdk up to 0.10.1. Affected by this vulnerability is an unknown functionality of the file src/mcp/index.ts of the component MCP Request Handler. The manipulation of the argument path results in server-side request forgery. The attack can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108773	A vulnerability was detected in erzhongxmu JEEWMS up to 2026.09.27-W39. Impacted is the function docheck of the file src/main/java/com/zzjee/wm/controller/WmOmNoticeHController.java. Performing a manipulation of the argument goodscode results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108774	A flaw has been found in erzhongxmu JEEWMS up to 2026.09.27-W39. The affected element is the function getbinall/getbinallagv of the file src/main/java/com/zzjee/md/controller/MdBinController.java. Executing a manipulation of the argument binstore/binid/des/cengshu can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108775	A vulnerability has been found in erzhongxmu JEEWMS up to 2026.09.27-W39. The impacted element is the function WvNoticeController.list of the file com/zzjee/wmapi/controller/WvNoticeController.java of the component Search Endpoint. The manipulation of the argument searchstr leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108777	A vulnerability was found in erzhongxmu JEEWMS up to 2026.09.27-W39. This affects the function WvGiController.list of the file src/main/java/com/zzjee/wmapi/controller/WvGiController.java. The manipulation of the argument searchstr results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2026-108778	A vulnerability was determined in erzhongxmu JEEWMS up to 2026.09.27-W39. This impacts the function WmInQmlController.list of the file src/main/java/com/zzjee/wm/controller/WmInQmlController.java of the component Inbound Quality Check Pda Interface. This manipulation of the argument searchstr causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108779	A vulnerability was identified in erzhongxmu JEEWMS up to 2026.09.27-W39. Affected is the function WmSttInGoodsController.list of the file src/main/java/com/zzjee/wm/controller/WmSttInGoodsController.java. Such manipulation of the argument searchstr leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108781	A security flaw has been discovered in erzhongxmu JEEWMS up to 2026.09.27-W39. Affected by this vulnerability is the function WmToMoveGoodsController.list of the file src/main/java/com/zzjee/wm/controller/WmToMoveGoodsController.java of the component PDA Interface. Performing a manipulation of the argument searchstr results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108570	A security flaw has been discovered in Furion .NET Framework up to 4.9.9.95. This affects the function RunCompile of the file framework/Furion/ViewEngine/Engines/ViewEngine.cs of the component View Engine. The manipulation of the argument content results in improper neutralization of special elements used in a template engine. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108785	A flaw has been found in macrozheng mall up to 1.0.3. This issue affects the function JwtTokenUtil.refreshHeadToken of the file /admin/refreshToken of the component JwtAuthenticationTokenFilter. This manipulation of the argument token causes session expiration. The attack may be initiated remotely. The exploit has been published and may be used. Patch name: 9bfc2fd2c4aaa4ac519e9152e65d673a5380de1a. To fix this issue, it is recommended to deploy a patch.	6.3	More Details
CVE-2026-94246	The Wallet System for WooCommerce WordPress plugin before 2.8.0 does not verify that the wallet account named in a withdrawal submission belongs to the user making it, allowing any authenticated user, such as a subscriber, to file a withdrawal request against another user's wallet for an amount and a payout destination of their choosing, and to indefinitely prevent that user from submitting withdrawals of their own.	6.3	More Details
CVE-2026-62035	Subscriber Broken Access Control in AWS S3 for WordPress Plugin – Upcasted <= 3.1.0 versions.	6.3	More Details
CVE-2026-108782	A weakness has been identified in erzhongxmu JEEWMS up to 2026.09.27-W39. Affected by this issue is the function CommonServiceImpl.getAutoList of the file src/main/java/org/jeecgframework/core/common/service/impl/CommonServiceImpl.java of the component Autocomplete Handler. Executing a manipulation of the argument trem/searchField/entityName can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108824	A flaw has been found in DataEase up to 3.0.0. The impacted element is the function Utils.buildCalcField of the file io/dataease/engine/utils/Utils.java. This manipulation of the argument calculated field causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. Patch name: 8509e218e6c1f0080ee9e379f269b2104785ef7. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2026-108821	A security vulnerability has been detected in Tencent WeKnora up to 0.8.1. Impacted is the function validateSubquery of the file internal/utils/inject.go of the component SQL Validator. The manipulation leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.8.2 is recommended to address this issue. The identifier of the patch is d7ccd5ba517cc3968e6d5000a2ab0f4b51ef1dda. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-108816	A vulnerability was found in agno-agi agno up to 3.0.6. Affected by this vulnerability is the function run_python_code of the file python.py of the component PythonTools. The manipulation of the argument code results in code injection. The attack can be launched remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-106065	A heap-based buffer overflow was found in GIMP's PCX export plug-in. For images with extremely large width and height, buffer allocation uses overflowing 32-bit width * height arithmetic while subsequent GEGL operations use the full extent, after integer overflow in size calculation	6.3	More Details
	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, and Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72, an authenticated user who does not hold the "admin" or "sc_admin" Splunk roles could modify Splunk Secure Gateway alert and mobile-device recipient data in App Key Value Store (KV Store) collections that later alert and subscription workflows use. The vulnerability is possible		

CVE-2026-76280	because the affected collections allow unrestricted write access instead of limiting writes to authorized Splunk Secure Gateway workflows. For more information see About the app key value store (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/administer-the-app-key-value-store/about-the-app-key-value-store), KV store endpoint descriptions (https://help.splunk.com/en/splunk-enterprise/leverage-rest-apis/rest-api-reference/10.4/kv-store-endpoints/kv-store-endpoint-descriptions), and About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) in the Splunk documentation.	6.3	More Details
CVE-2026-108604	Tabularis through 0.27.0 contains an incorrect authorization vulnerability in the MCP run_query safety gate that allows prompt-injected agents or untrusted MCP clients to bypass read-only mode by submitting side-effecting SELECT statements. Attackers can run statements like SELECT setval, nextval, or PostgreSQL query_to_xml with embedded DELETE to modify data without approval prompts.	6.3	More Details
CVE-2026-108814	A flaw has been found in SEMCMS up to 5.0. This impacts an unknown function of the file SEMCMS_Banner.php. Executing a manipulation can lead to sql injection. 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.	6.3	More Details
CVE-2026-108813	A vulnerability was detected in SEMCMS up to 5.0. This affects an unknown function of the file SEMCMS_Download.php. Performing a manipulation results in sql injection. 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.	6.3	More Details
CVE-2026-108538	A security vulnerability has been detected in GPAC up to 26.07.0. The impacted element is the function gf_mx_v of the file utils/os_thread.c of the component MP4Box. Such manipulation leads to use after free. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108539	A vulnerability was detected in GPAC up to 26.07.0. This affects the function gf_fq_pop of the file filter_core/filter_queue.c of the component MP4Box. Performing a manipulation results in use after free. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-87681	An Access Control Bypass vulnerability exists in the Role-Based Access Control (RBAC) validation engine of Brocade Fabric OS versions before 10.0.1. When processing certain management protocol operations, the RBAC engine incorrectly categorizes non-standard action opcodes during permission checks. This allows authenticated users with read-only management privileges to bypass access controls and execute restricted administrative operations.	6.3	More Details
CVE-2026-108541	A vulnerability has been found in highwarden Super Store Finder up to 3.8. Affected is an unknown function of the file /products/superstorefinder/index.php. The manipulation of the argument lat/lng leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. Upgrading to version 3.9 is able to address 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.	6.3	More Details
CVE-2026-78018	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Initialization of a Resource with an Insecure Default vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	6.3	More Details
CVE-2026-108820	A weakness has been identified in agno-agi agno up to 3.0.6/3.1.1. This issue affects the function member_agent.run in the library libs/agno/agno/team/_default_tools.py of the component Delegation Feature. Executing a manipulation can lead to execution with unnecessary privileges. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.	6.3	More Details
CVE-2026-108803	A security vulnerability has been detected in y_project RuoYi up to 4.8.3. This impacts the function changeStatus of the file /system/config/add of the component Disable API. The manipulation leads to session expiration. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-108831	A security vulnerability has been detected in meetecho janus-gateway up to 1.4.2. This vulnerability affects unknown code of the file html/demos/admin.js of the component Admin API. Such manipulation leads to hard-coded credentials. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-78340	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Filesystem access for attacker.	6.3	More Details

CVE-2026-108801	A security flaw has been discovered in prasathmani TinyFileManager up to 2.6. The impacted element is the function move_uploaded_file of the file tinyfilemanager.php. Performing a manipulation of the argument fullpath results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-78339	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure, Protection mechanism bypass, and Unauthorized access.	6.3	More Details
CVE-2026-107391	music-metadata is a metadata parser for audio and video media files. In the public development revision introduced after 11.14.0, a development-branch regression in the MP4 stsd sample-description parser allows an attacker-controlled sample-entry size of zero to prevent the StsdAtom.get cursor from advancing while an attacker-controlled entry_count keeps the synchronous loop running. A crafted MP4-family input can block the Node.js event loop and grow the sample-description table until the process is terminated or exhausts memory. The vulnerable change was present on the public master branch but was not included in music-metadata 11.14.0 or any earlier npm release, and version 11.16.0 contains the fix. This issue is fixed in version 11.16.0.	6.2	More Details
CVE-2026-107169	A flaw was found in m17n-lib. An attacker could provide specially crafted or truncated UTF-8 input to trigger an unhandled null pointer dereference during text processing. This issue causes the application to crash unexpectedly, resulting in a Denial of Service (DoS).	6.2	More Details
CVE-2026-107437	GV-E-Map Server V18.2.0A contains a plaintext database password embedded within an application component. The credential can be recovered through static analysis of the distributed binary and may also be exposed in process memory during runtime.	6.2	More Details
CVE-2026-107392	music-metadata is a metadata parser for audio and video media files. Prior to 11.15.0, the DSF parser handles an unrecognized chunk by calling tokenizer.ignore without awaiting the returned promise and without first rejecting a chunk size smaller than the 12-byte chunk header. A crafted DSF input can produce a negative ignore length; with strtok3 10.3.5 or later, the resulting RangeError is detached from the parseBuffer promise and becomes an unhandled rejection under Node.js default behavior. The parse call can appear to resolve before the process crashes, bypassing per-parse try/catch handling. The demonstrated impact is availability loss only and requires the DSF parsing path. This issue is fixed in version 11.15.0.	6.2	More Details
CVE-2026-107167	A flaw was found in m17n-lib. A user providing specially crafted text input can trigger a heap use-after-free condition during input-method state transitions. Under specific conditions, the library frees an internal input context object but subsequently attempts to write to that freed memory. This issue can cause applications relying on the library to crash, leading to a Denial of Service (DoS), or potentially allow arbitrary code execution.	6.2	More Details
CVE-2026-107388	music-metadata is a metadata parser for audio and video media files. Prior to 11.16.0, the ID3v2 parser trusts the synsafe tag-size field and allocates the complete tag body before checking whether the input contains the declared bytes. A truncated file containing only an ID3v2 header can request an allocation approaching 268 MiB; the allocation succeeds, the subsequent read reaches end of stream, the EndOfStreamError is caught internally, and the caller receives a normal metadata object. This issue is fixed in version 11.16.0.	6.2	More Details
CVE-2026-106579	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31 and 6.9.13-56, a crafted image can bypass an ImageMagick security policy that uses coder as its domain, potentially allowing data prohibited by the policy to be read. This issue is fixed in versions 7.1.2-31 and 6.9.13-56.	6.2	More Details
CVE-2026-107387	music-metadata is a metadata parser for audio and video media files. Prior to 11.16.0, the APEv2 parser reads an attacker-controlled tag-item size and allocates a Uint8Array for a binary item before proving that the declared item fits in the remaining tag or file data. A small crafted APE file can therefore trigger a disproportionate allocation, including through cover-art items, and repeated or concurrent parsing can exhaust process memory. The demonstrated impact is availability loss only. This issue is fixed in version 11.16.0.	6.2	More Details
CVE-2026-107389	music-metadata is a metadata parser for audio and video media files. Prior to 11.16.0, the Matroska and WebM EBML parser decodes an attacker-controlled VINT element length and uses it for string-token or Uint8Array allocation before confirming that the leaf fits within its parent or available input. Crafted WebM, MKV, or MKA inputs can cause disproportionate allocations, out-of-memory denial of service, or, for a demonstrated parseFile path on Node.js 26.7.0, an uncatchable V8 fatal abort. The exact failure mode depends on the tokenizer, parser API, and runtime, but the affected leaf-length validation flaw is shared and has availability impact only. This issue is fixed in version 11.16.0.	6.2	More Details
CVE-2026-107168	A flaw was found in m17n-lib. By providing crafted input containing an invalid UTF-8 character sequence, an attacker can cause the text parsing function to enter an infinite loop. This issue leads to sustained high CPU utilization, resulting in a Denial of Service (DoS) for the affected application.	6.2	More Details

CVE-2026-107390	music-metadata is a metadata parser for audio and video media files. Prior to 11.16.0, the MP4 parser accepts an attacker-controlled 64-bit extended atom size, converts it to a JavaScript Number, and uses the resulting payload length for atom-specific readToken calls before proving that the atom fits within its parent or the available input. A tiny MP4-family file can route an oversized length into payload parsing for atoms including mvhd, stsd, stsz, and date, causing a large allocation attempt or process failure before end-of-input validation. Applications that parse untrusted MP4-family media can therefore be denied service. This issue is fixed in version 11.16.0.	6.2	More Details
CVE-2026-106437	The BSON buffer-reservation API in the MongoDB C Driver can record a length smaller than the five-byte BSON minimum. Later append or comparison operations can underflow unsigned length calculations and read or write outside the document buffer. An actor who can influence the length supplied by an embedding application can cause the application to terminate or read or corrupt adjacent process memory. Reaching this issue requires the application to pass an undersized value to bson_reserve_buffer and then perform an affected operation.	6.2	More Details
CVE-2026-105829	League CommonMark from 1.3.0 before 2.10.2 contains a cross-site scripting vulnerability that allows users posting Markdown to bypass the DisallowedRawHtml extension by ending raw HTML with a bare disallowed tag name. Attackers can place a lone <script or <iframe line followed by a block supplying attributes like src or onload, executing stored scripts in viewers' browsers under default GFM settings.	6.1	More Details
CVE-2026-104083	SmarterMail before build 9777 contains a stored mutation cross-site scripting vulnerability that allows remote attackers to inject executable script by placing payloads inside a <style> element nested within MathML foreign content (<math><mtext><mglyph>), which the custom HTML sanitizer treats as inert CDATA text but browsers reparse as live markup. Attackers can deliver a crafted calendar (iCal) message containing an payload that executes automatically in the recipient's webmail session at /interface/message-iframe when the message is opened, enabling script execution and data exfiltration unconstrained by the interface's permissive Content-Security-Policy.	6.1	More Details
CVE-2026-107797	JiveJdon through 5.0 contains a reflected cross-site scripting vulnerability in application/message/postThread.jsp that allows attackers to inject script via the to and tag parameters. Attackers can send crafted links to authenticated users, breaking out of unencoded inline JavaScript string literals to execute arbitrary JavaScript in the victim's session.	6.1	More Details
CVE-2026-89100	The Payment Plugins for Stripe WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via '#response' URL Fragment in all versions up to, and including, 4.0.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that the 'Generic Errors' setting is unchecked, causing getErrorMessage() to return the raw Stripe error string unchanged rather than substituting a mapped safe message.	6.1	More Details
CVE-2026-107718	AdonisJS HTTP Server is a package for handling HTTP requests in the AdonisJS framework. Prior to 8.2.3 and 9.3.0, AdonisJS HTTP Server inserts route parameter values into URLs without encodeURIComponent in the shared createURL() helper used by Router.makeUrl() and Response.redirect().toRoute(). If an application places attacker-controlled data in a dynamic first path segment and uses the generated route URL as a redirect destination, a value beginning with a slash can produce a scheme-relative external URL. Wildcard parameters are affected by the same missing encoding, while APIs intentionally accepting complete redirect URLs are not affected. An attacker can redirect users from a trusted application to an attacker-controlled site, facilitating phishing or abuse of authentication and OAuth flows. This issue is fixed in versions 8.2.3 and 9.3.0.	6.1	More Details
CVE-2026-107393	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.235, when APP_CLOUDFLARE_IS_USED is enabled, FreeScout trusts an unvalidated CF-Connecting-IP header during failed login attempts and stores the spoofed value in the activity log. LogsMonitor inserts the value into an administrator alert email without HTML escaping, allowing injected HTML to execute when an administrator opens the email. This issue is fixed in version 1.8.235.	6.1	More Details
CVE-2026-108925	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Cohesity NetBackup Administration Console web interface. This issue affects NetBackup Administration Console web interface: versions before 11.2. https://github.com/cohesity/SecAdvisory/blob/master/COH-2026-0002.md	6.1	More Details
CVE-2026-107634	Dislocker through 0.7.3 contains a heap out-of-bounds read vulnerability in get_dataset() and get_next_datum() that never validate dataset and datum sizes against the metadata allocation. Attackers can craft a BitLocker volume image with inflated dataset or datum sizes that, when opened or mounted, crashes dislocker or discloses adjacent heap memory.	6.1	More Details
CVE-2026-107614	An integer underflow in WinCursorShapeUtils::trimTransparent() in GlavSoft TightVNC Server for Windows before 2.8.88 allows a local authenticated user to crash the server, and potentially read out-of-bounds memory, by causing a cursor shape with a width or height of zero to be processed on the DXGI capture path. The loop bound width - 1 wraps to 0xFFFFFFFF, producing an access roughly 4 GB beyond the 64 KB cursor buffer; a monochrome cursor of height 1 also becomes 0 because getCursorHeight() halves the height in place.	6.1	More Details

CVE-2026-5725	The Favicon Rotator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'fvrt_' prefixed request parameters in all versions up to, and including, 1.2.11 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-2025-70519	The device log component of Fanvil x7a firmware version 2.6.0.1182 does not properly sanitize or encode reflected user supplied data. The lack of sanitization allows for the injection of HTML which can be used to execute malicious JavaScript code on any target browser which renders the device log component.	6.1	More Details
CVE-2026-93581	User-controlled values are not sufficiently neutralized when included in CSV exports. Values originating from user input, including data submitted by authenticated users or received through external communication channels such as email, may be stored in fields that are later included in CSV exports. An attacker can therefore inject values beginning with spreadsheet formula characters such as =, +, -, or @. An attacker does not necessarily require an authenticated account if the affected field can be populated through an external input channel such as incoming email. When an affected CSV file is opened in spreadsheet software, the application may interpret these values as formulas instead of plain text. Depending on the spreadsheet application and its security configuration, a malicious formula may cause unintended actions, disclose information, or invoke external functionality. Exploitation may require the user opening the exported CSV file to confirm one or more security warning dialogs. The vulnerability does not execute code on the OTRS server; any additional impact occurs in the spreadsheet application used to process the exported file. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	6.1	More Details
CVE-2026-107466	A flaw was found in flatpak-builder. This vulnerability allows an attacker to cause information disclosure by convincing a user or continuous integration (CI) system to process a crafted build manifest. By specifying local file Uniform Resource Identifiers (URIs) within source download definitions, the builder bypasses directory confinement checks. As a result, sensitive host files accessible to the build process can be read and incorporated into the build artifacts.	6.1	More Details
CVE-2026-94154	The Aurora Heatmap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 1.7.2 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 an admin user clicks the injected heatmap link.	6.1	More Details
CVE-2026-103998	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'inputs (array key)' parameter in all versions up to, and including, 1.15.48 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-2026-107796	Jivejdon from commit 5489372d through commit ee67a65e contains a reflected cross-site scripting vulnerability in application/query/taggedThreadList.jsp that allows unauthenticated attackers to inject script via unencoded tagID and count parameters. Attackers can craft a link with a script-closing payload in tagID or count, triggered when start exceeds zero, to execute JavaScript in victims' browsers.	6.1	More Details
CVE-2026-87869	The Filter Everything — WordPress & WooCommerce Filters plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in versions up to, and including, 1.9.6. This is due to insufficient input sanitization and output escaping in the flrt_elementor_load_more_anchor() function. The function reads query parameters from \$_SERVER['REQUEST_URI'] via getFormActionOrFullPageUrl(true), which URL-decodes them through parse_str() and re-assembles them using build_query() — a WordPress core function that does NOT re-encode values (\$urlencode=false). The resulting URL, containing unescaped special characters, is injected into a data-next-page HTML attribute via preg_replace() without esc_attr() or esc_url(). 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 specially crafted link.	6.1	More Details
CVE-2026-12054	The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'REFERRER' parameter in all versions up to, and including, 3.3.57 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute in a victim's browser.	6.1	More Details
CVE-2026-102258	Post-authentication Stored Cross-Site Scripting (XSS) vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to store and potentially execute arbitrary JavaScript code in the Appliance Management Console (AMC).	6.1	More Details
CVE-2026-32645	Default factory credentials with administrative access are enabled and persist even after configuring other administrator accounts.	6.0	More Details
CVE-	Missing authentication has been found in remote-execution task updates in the smart_proxy_dynflow package. The progress and completion callbacks accept a report when the one-time token is missing. A		More

2026-107151	network attacker or user must already know the identifier of a running job. This applies when remote execution is set to pull or pull-mqtt mode. They can send their own job output and mark the job as a success or a failure. The job is then recorded with that result.	5.9	Details
CVE-2026-107325	Improper validation of a BSON array length in the MongoDB Go Driver can cause an out-of-bounds index and runtime panic when an application calls bson.RawArray.Validate or bsoncore.Array.Validate on a malformed four-byte array. An unauthenticated actor who can supply raw BSON array data to an affected application may terminate an unprotected application process, causing a denial of service. No confidentiality or integrity impact has been identified.	5.9	More Details
CVE-2026-79363	Cloudron 9.1.7 and 9.2 contain a stored cross-site scripting (XSS) vulnerability in the Branding Footer feature. An authenticated administrator can store crafted HTML containing JavaScript event handlers in the Footer setting. The stored value is rendered without sufficient sanitization on the public login / OpenID interaction page and in the System Event Log, causing attacker-controlled JavaScript to execute in the Cloudron web origin when an affected page is viewed.	5.9	More Details
CVE-2026-107177	Express Gateway through 1.16.11 contains a hardcoded cryptographic key vulnerability that allows attackers with datastore access to decrypt stored OAuth 2.0 token secrets via the default crypto.cipherKey 'sensitiveKey'. Attackers who can read Redis can decrypt tokenEncrypted values and combine them with stored token IDs to obtain valid bearer tokens for any user.	5.9	More Details
CVE-2026-19498	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote attacker to cause a denial of service due to uncontrolled recursion.	5.9	More Details
CVE-2026-108105	Open5GS through 2.8.0 contains a reachable assertion vulnerability in mme_gn_handle_sgsn_context_request() that allows remote unauthenticated attackers to crash the MME via malformed SGSN Address IEs. Attackers sending GTPv1-C traffic from a configured SGSN address with a known UE IMSI or P-TMSI can supply an invalid address length to terminate open5gs-mmed, denying service to all subscribers.	5.9	More Details
CVE-2026-42419	Unauthenticated Sensitive Data Exposure in Swish Migrate and Backup <= 1.4.0 versions.	5.9	More Details
CVE-2026-107285	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.12 and 2.16.1, a proxied ws request is carried through CONNECT, but NettyRequestFactory.newNettyRequest and requestUri decide whether to attach proxy authentication and an absolute-form target only from whether the URI is secure. Because ws is not marked secure, the tunneled WebSocket upgrade sent to the origin includes the proxy's Proxy-Authorization value. Basic credentials are directly recoverable and Digest responses can be replayed or cracked offline. This issue is fixed in versions 3.0.12 and 2.16.1.	5.9	More Details
CVE-2026-107324	An integer overflow in BSON value-length handling in the MongoDB Go Driver can cause a runtime panic when an application validates or accesses a malformed BSON document. An unauthenticated actor who can supply BSON bytes to an affected application may terminate an unprotected application process, causing a denial of service. The driver's server-monitoring path contains panic recovery and is limited to server-selection failure.	5.9	More Details
CVE-2026-107382	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. From 3.3.0 until 3.5.4, the zero-configuration TLS fingerprint-validation path calls Ed25519PasswordAuth.hash() through Authentication.validateFingerPrint, but Ed25519PasswordAuth.hash() references a seed identifier that is not in scope. Exposure requires a MariaDB server reached over TCP, TLS enabled with ssl: true or an ssl object whose rejectUnauthorized value is not false, a password set, no ssl.ca configured, and client_ed25519 negotiated as the authentication plugin. Under those conditions, a legitimate server, malicious server, or network attacker presenting a self-signed certificate can reach this path and cause a synchronous ReferenceError to escape the socket data handler. Under Node.js default uncaught-exception behavior, the client process terminates, causing denial of service. Configurations using a provided CA, rejectUnauthorized: false, another authentication plugin, or a Unix socket do not reach this vulnerable path. This issue is fixed in version 3.5.4.	5.9	More Details
CVE-2026-107829	Jivejdon through 5.0 contains a weak password storage vulnerability that stores account passwords as unsalted MD5 digests via ToolsUtil.hash() in AccountDaoSql. Attackers who obtain the user table through database access or SQL injection can crack passwords with precomputed tables or GPU attacks.	5.9	More Details
CVE-2026-59508	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Interuse i-Bos. This issue affects i-Bos: 3.0.	5.9	More Details
	pgjdbc, the PostgreSQL JDBC Driver, versions 42.7.11 through 42.7.13 enforce no restriction when the requireAuth connection property excludes all six authentication methods the driver knows, for example requireAuth=!password,!md5,!gss,!sspi,!scram-sha-256,!none. The driver then accepts any method the		

CVE-2026-107314	server asks for, including cleartext password authentication. A value without a method in it, such as requireAuth=, (a single comma), is affected the same way. An attacker positioned between the application and its server can ask for cleartext password authentication and receive the database password. A positive list such as requireAuth=scram-sha-256, and a partial exclusion such as requireAuth=!password,!md5, are enforced correctly. The property has no default value, so a deployment that does not set it is not affected. 42.7.14 fixes the problem: such a connection is refused with SQLState 08004, and a value without a method in it is rejected as invalid.	5.9	More Details
CVE-2026-103323	The Integration for Epos Now and WooCommerce WordPress plugin before 4.11.2 does not perform an authorization check on one of its REST endpoints, allowing unauthenticated users to retrieve the site's scheduled background tasks and their arguments, which include order identifiers and, when WooCommerce's deferred emails feature is enabled, the plaintext passwords of newly registered customers.	5.9	More Details
CVE-2024-8122	The WSO2 Identity Server fails to enforce a default expiry time for SMS One-Time Passwords (OTPs) used in multi-factor authentication (MFA). This allows unused OTPs to remain valid indefinitely, presenting an opportunity for malicious actors to conduct brute force attacks by repeatedly guessing the OTP. The absence of automatic expiration for OTPs grants attackers an unlimited timeframe to attempt guessing the correct code. A successful brute force attack can lead to an MFA bypass, resulting in the unauthorized takeover of a user's account and compromising the security and privacy of both the individual and the system.	5.9	More Details
CVE-2026-108729	Corteza through 2024.9.10 contains an incorrect authorization vulnerability in compose attachment endpoints that allows unauthenticated attackers to download private attachments by setting the URL kind segment to page, icon, or namespace. Attackers who know a private record or module attachment id can request the original or preview route without a token or signature to retrieve files across namespace and record permission boundaries.	5.9	More Details
CVE-2026-107783	Insertion of sensitive information into log file in AWS Tools for PowerShell before 5.0.306 might allow local users to recover an IAM user's cleartext AWS Management Console password from command output and log artifacts. To remediate this issue, users should upgrade to version 5.0.306 or later. After upgrading, review PowerShell transcripts and log stores for previously disclosed passwords and rotate any affected IAM console passwords.	5.9	More Details
CVE-2026-16182	IBM DataPower Gateway 10.5.0.0 through 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow an attacker to cause a denial of service due to a NULL pointer dereference in GraphQL variable processing.	5.9	More Details
CVE-2026-105818	Vault's PKI secrets engine ACME server did not restrict certificate identities that ACME challenges do not validate when issuing certificates under the default directory policy. This may allow an ACME client to obtain a certificate containing unverified identity claims, potentially enabling impersonation toward systems that trust certificates issued by the affected Vault PKI mount. This vulnerability (CVE-2026-105818) is fixed in Vault Community Edition 2.1.2, and Vault Enterprise 2.1.2, 1.21.12, 1.20.17, and 1.19.23.	5.9	More Details
CVE-2026-106430	The MongoDB C++ Driver discards content after an embedded NUL byte in certain field and collection names accepted by the collection API. This can cause the driver and the calling application to interpret the same name differently. An authenticated actor who can influence a name passed by an affected application can cause the application to read distinct values from an unintended field or rename an unintended collection. These operations use the application's existing database credentials.	5.9	More Details
CVE-2026-107675	FFmpeg through 9.0.2 contains a missing host key verification vulnerability in the libssh-based sftp protocol handler that allows network attackers to impersonate SFTP servers. Attackers performing man-in-the-middle, DNS, or ARP spoofing can capture passwords supplied in sftp URLs, serve forged media, or receive uploaded output.	5.9	More Details
CVE-2026-107833	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. From 3.0.0 until 3.8.0, ProcessResponse in internal/bodyprocessors/json.go passes the ignoreJSONRecursionLimit value of -1 to readJSON, while the recursive guard only stops at zero. A network attacker who can cause an application protected by Coraza to return deeply nested JSON can make response-body processing perform quadratic work, consuming one CPU core for seconds per response within the default ResponseBodyLimit. Request JSON processing is not affected by this specific path because it uses the configured request recursion limit, and exploitation requires response-body inspection to be enabled. This issue is fixed in version 3.8.0.	5.9	More Details
CVE-2026-107819	MariaDB Connector/C is a C and C++ client library for connecting applications to MariaDB and MySQL databases. From 3.4.1 until 3.4.10, the MariaDB Connector/C libmariadb Zero-Configuration SSL authentication-switch logic checked certificate trust failure but did not reject a TLS hostname verification mismatch before selecting a non-hashing authentication plugin. An active man-in-the-middle attacker with a valid certificate for another hostname could request mysql_clear_password and obtain the database password inside the attacker-controlled TLS connection. Other MariaDB connectors are not affected. This issue is fixed in version 3.4.10.	5.9	More Details
CVE-2026-106565	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32 and 6.9.13-57, a missing end-of-file check while reading bzip2-compressed image data can cause an infinite loop and exhaust processing resources. This issue is fixed in versions 7.1.2-32 and 6.9.13-57.	5.9	More Details

CVE-2026-107714	The Mechanize library is used for automating interaction with websites. Prior to 2.14.1, Mechanize::HTTP::Agent#response_redirect treats redirects as same-origin when the host matches without consistently comparing scheme and port. A same-host HTTPS-to-HTTP redirect can send Authorization and Cookie headers over cleartext, while a same-host redirect to another port can send a caller-supplied Cookie header to a different service. Cookies in Mechanize#cookie_jar remain scoped separately; the issue affects caller-supplied headers and can disclose credentials without affecting integrity or availability. This issue is fixed in version 2.14.1.	5.9	More Details
CVE-2026-84891	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a remote attacker to obtain sensitive information due to use of hard-coded credentials.	5.9	More Details
CVE-2026-107299	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, the streaming decoder treats the reserved MessagePack byte 0xc1 as incomplete input instead of invalid input. When 0xc1 begins a stream, subsequent data remains buffered while the decoder waits for bytes that cannot make the value valid, allowing a remote peer to exhaust memory. This issue is fixed in version 6.1.0.	5.9	More Details
CVE-2026-107297	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, the streaming decoder reparses an incomplete array or map from the beginning whenever another chunk arrives. A remote peer can split one valid MessagePack container across many small chunks, causing completed elements to be decoded repeatedly, producing quadratic CPU use and blocking the event loop. This issue is fixed in version 6.1.0.	5.9	More Details
CVE-2026-106567	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32 and 6.9.13-57, a crafted PSD file can trigger an integer-conversion error in the PSD decoder on 32-bit builds, causing an infinite loop and denial of service. This issue is fixed in versions 7.1.2-32 and 6.9.13-57.	5.9	More Details
CVE-2026-106578	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31 and 6.9.13-56, a crafted image can cause an invalid memory free in the MVG decoder and crash the process. This issue is fixed in versions 7.1.2-31 and 6.9.13-56.	5.9	More Details
CVE-2026-96518	Missing Authorization vulnerability in properfraction ProfilePress wp-user-avatar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ProfilePress: from n/a through 4.17.3.	5.9	More Details
CVE-2026-66435	Insertion of Sensitive Information Into Sent Data vulnerability in Devin Walker WP Rollback wp-rollback allows Retrieve Embedded Sensitive Data.This issue affects WP Rollback: from n/a through 3.1.2.	5.9	More Details
CVE-2026-107209	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-30 and 6.9.13-55, when ImageMagick is built without Cairo support, a crafted RSVG image that reaches a resource limit can cause the RSVG decoder to free image state twice and then use freed memory, crashing the process. This issue is fixed in versions 7.1.2-30 and 6.9.13-55.	5.9	More Details
CVE-2026-108545	SillyTavern 1.12.13 through 1.19.0 contains a denial of service vulnerability that allows unauthenticated remote attackers to exhaust resources because body-parser middleware runs before authentication and whitelist checks. Attackers can send large or compressed JSON or urlencoded bodies up to 500 MB, optionally in parallel, to exhaust memory and CPU and deny service.	5.9	More Details
CVE-2026-107613	A NULL pointer dereference vulnerability in the Win8ScreenDriver component of GlavSoft TightVNC Server for Windows before 2.8.88 allows an attacker to crash the server, causing a denial of service. When re-initialization of the DXGI Desktop Duplication driver fails in applyNewScreenProperties() (for example after a GPU reset, display hot-plug or session change), m_drvImpl is left NULL and is subsequently dereferenced without a check by executeDetection(), getScreenBuffer(), grabFb(), getScreenPropertiesChanged() and getCursorPosition().	5.9	More Details
CVE-2026-11930	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 may not enforce authorization correctly for some web servers.	5.9	More Details
CVE-2026-14509	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote attacker to cause a denial of service due to algorithmic complexity in linked-list traversal.	5.9	More Details
CVE-2026-107721	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.3.0, fast-jwt createVerifier accepts Infinity for clockTolerance because its option validation checks type and negativity but not finiteness. In validateClaimDateValue, infinite positive and negative modifiers make exp and nbf comparisons always pass, allowing expired or not-yet-active tokens to be accepted. The verifier cache also derives infinite bounds, so entries created under this configuration can remain valid until eviction. Exploitation requires an application administrator or equivalent configuration path to set clockTolerance to Infinity. This issue is fixed in version 6.3.0.	5.9	More Details
	Improper certificate validation in the webmail of Progressive Robot hMailServer 6.3.2 through 6.3.5 allows a remote unauthenticated attacker to have S/MIME-encrypted mail that the account later sends to another		

CVE-2026-107587	correspondent also encrypted to the attacker's key. When its recipient opened a signed message, the webmail kept the signer's certificate for encrypting replies whether or not the server found its chain trusted, under the first e-mail address the certificate listed rather than the message's From address, and beside any certificate already held for that address. Encrypted mail later sent from the webmail to that address was encrypted to every certificate held for it, so a holder of the kept certificate's key who obtains a copy of such a message can read it.	5.9	More Details
CVE-2026-86826	The BackWPup WordPress plugin before 5.7.7 does not properly restrict web access to the working directory it uses during backup restores, allowing unauthenticated attackers, on web servers that do not honour .htaccess rules such as NGINX, to download the full backup archive (database dump and site files, including credentials and secret keys) left behind by an interrupted restore.	5.9	More Details
CVE-2026-20038	A vulnerability in the endpoint group (EPG) contract functionality of Cisco Nexus 9000 Series Fabric Switches in ACI Mode could allow an unauthenticated, remote attacker to bypass configured EPG contracts. This vulnerability is due to an improper control with EPG contracts. An attacker could exploit this vulnerability by sending IPv4 or IPv6 packets using UDP source and destination ports that are assigned to DHCP traffic through an affected device. A successful exploit could allow the attacker to bypass EPG contracts on the affected device.	5.8	More Details
CVE-2026-78027	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Server-Side Request Forgery (SSRF) vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and Server-side request forgery.	5.8	More Details
CVE-2026-20173	A vulnerability in Cisco NX-OS Software could allow an unauthenticated, remote attacker to exhaust system resources, causing a denial of service (DoS) condition. This vulnerability exists because rate limiting was improperly applied to some protocols. An attacker could exploit this vulnerability by sending a high rate of UDP or TCP connections to a data plane interface on an affected device. A successful exploit could allow the attacker to cause instability to various routing and control plane protocols through some packet loss and temporary disruptions, causing a DoS condition. This DoS condition will clear without manual intervention soon after the high rate of traffic is stopped.	5.8	More Details
CVE-2026-107841	pacioli provides least-privilege governance and a governed agent broker for ERPNext. From version 0.9.6 until version 0.10.0, the pacioli-guard document-layer consent gate allows nested cancellation operations to ride any consent established by an enclosing governed act without checking whether the marker authorizes cancellation. A credential with API Key Scope.require_consent can submit a caller-controlled Sales Invoice or other supported document under a valid human-minted submit marker and reach Document.cancel() for a different pre-existing submitted document, bypassing the marker's document and act binding, single-use spend, and denial audit. The unauthorized cancellation can reverse the target document's ledger effect; principals without a consent-gated grant are not affected. This issue is fixed in version 0.10.0.	5.7	More Details
CVE-2026-108501	ZTE Z80 Ultra has a system interface permission verification defect. The interface lacks necessary access control, and relevant information can be read by reflectively invoking the interface.	5.7	More Details
CVE-2026-106431	An off-by-one error in the BSON bulk document writer in the MongoDB C Driver can write one zero byte immediately past a heap allocation when a document ends at a specific buffer boundary. An actor who can influence the size of documents serialized by an embedding application can corrupt adjacent process memory or terminate the process. Reaching this issue requires the application to use the BSON bulk-writer API and produce a precise cumulative document size.	5.7	More Details
CVE-2026-84032	IBM Guardium Data Protection 12.2.2 could allow a remote attacker to conduct a man-in-the-middle attack due to improper certificate validation.	5.6	More Details
CVE-2026-96334	Missing Authorization vulnerability in ThemeGrill User Registration user-registration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Registration: from n/a through 5.2.7.	5.6	More Details
CVE-2026-96539	Incorrect Privilege Assignment vulnerability in Ultimate Member Ultimate Member ultimate-member allows Privilege Escalation.This issue affects Ultimate Member: from n/a through 2.13.1.	5.6	More Details
CVE-2026-107635	Dislocker through 0.7.3 contains an integer underflow vulnerability in get_vmk() and get_fvek() that allows attackers to trigger out-of-bounds heap reads via crafted datum sizes. Attackers can supply a malicious BitLocker volume image with a datum_size smaller than the 36-byte AES-CCM header, causing hexdump() to over-read and crash dislocker.	5.5	More Details
CVE-2026-108978	Heap-based buffer overflow vulnerability in Samsung Opensource rlottie allows Buffer Overflow via Environment Variables. This issue affects rlottie: e57b094f03c39a751a1fded6f7d6c13f1ed95ec9.	5.5	More Details
CVE-2026-	ZTE Z80 Ultra has an unauthorized information disclosure vulnerability. The access control for methods within	5.5	More

108504	the framework is insufficient. An attacker can exploit this method to read device-related information.		Details
CVE-2026-44036	Uncontrolled mutual recursion between DcmXMLParseHelper::parseDataSet() and DcmXMLParseHelper::parseSequence() in the XML-to-DICOM converter (dcmdata/libdcxml/xml2dcm.cc) of OFFIS DCMTK 3.7.0 allows an attacker to cause a denial of service (stack exhaustion and process crash) via a crafted XML file with deeply nested sequence and item elements. The xml2dcm tool and any service that converts untrusted XML to DICOM with this code are affected. The issue is fixed in commit 87f256d73e30656a822bf7d76d1cf1d9bb693954.	5.5	More Details
CVE-2026-44037	Uncontrolled mutual recursion between DcmJSONReader::parseDataSet(), DcmJSONReader::parseElement() and DcmJSONReader::parseSequence() in dcmdata/libsrc/dcjsonrd.cc of OFFIS DCMTK 3.7.0 allows an attacker to cause a denial of service (stack exhaustion and process crash) via a crafted DICOM JSON document with deeply nested sequence (SQ) values. The json2dcm tool and any service that converts untrusted DICOM JSON (for example, DICOMweb payloads) with this reader are affected. The issue is fixed in commit cf955e64c35a1e07ba10698f639d5dcdec53b9d7.	5.5	More Details
CVE-2026-108506	ZTE Z80 Ultra's system interfaces do not have robust invocation authentication, with inadequate access control. Third-party apps may call the interfaces through reflection and retrieve relevant information.	5.5	More Details
CVE-2026-108817	A vulnerability was determined in agno-agi agno up to 3.0.9. Affected by this issue is the function agno.CodingTools.run_shell in the library libs/agno/agno/tools/coding.py of the component CodingTools. This manipulation of the argument command causes os command injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 3.0.10 can resolve this issue. Patch name: ed64fab5be63d2b15faddc2ef7c733176daa14aa. You should upgrade the affected component.	5.5	More Details
CVE-2026-106061	A flaw was found in GIMP's X cursor (XMC) thumbnail loader. When GIMP generates a thumbnail for a crafted XMC file, it allocates a pixel buffer using a width * height size computed in 32-bit signed arithmetic. If that product overflows, the allocation is smaller than the true image extent. A subsequent GEGL buffer read uses the unwrapped dimensions and performs an out-of-bounds read on the heap, after integer overflow in the size calculation. This can crash GIMP or corrupt process memory.	5.5	More Details
CVE-2026-42532	A path traversal vulnerability exists in the EmailSheet extract_parts functionality of VisiData (version(s): dev (commit 38b21f78)). A specially crafted .eml file can lead to arbitrary file write. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2026-61801	The `github.com/moby/sys/user` package provides Go utilities for parsing and looking up entries in Unix-style user and group database files. Versions before 0.4.1 do not sufficiently limit entries when parsing `/etc/passwd` - or `/etc/group` -style files, allowing an attacker who can supply a specially crafted file to cause excessive memory consumption and potentially terminate the affected process due to an out-of-memory condition. This issue is patched in version 0.4.1. As a workaround, avoid parsing attacker-controlled user or group database files, or validate and limit untrusted input before parsing it.	5.5	More Details
CVE-2026-107731	SumatraPDF is a multi-format reader for Windows. In 3.7.0.22298, four independently reachable range-validation variants in src/LitDoc.cpp allow file-controlled offsets and sizes to overflow, narrow to negative values, or wrap before incomplete bounds checks. The affected calculations include contentOffset, the directory expression dirOff64 + dirLen64, and the decoded-section offset + size, along with secondary-header range handling. Opening a crafted LIT file that reaches one of these variants can cause invalid pointer reads and deterministic application termination. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	5.5	More Details
CVE-2026-107332	Insecure file permissions in the CodeCatalyst connection handler in AWS Toolkit for VS Code before 4.10.0 allowed local users to obtain CodeCatalyst bearer tokens via reading world-readable token cache files. To mitigate this issue, users should upgrade to version 4.10.0 or later.	5.5	More Details
CVE-2026-12109	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow an attacker with administrative privileges and access to the local management interface to execute arbitrary code due to an unbounded write to a fixed-size stack buffer.	5.5	More Details
CVE-2026-107651	A flaw was found in Eye of GNOME (eog). A heap-based buffer overflow exists in the PNG metadata reader due to improper state handling when parsing split metadata chunks. A remote attacker could exploit this flaw by enticing a user into opening a specially crafted PNG file, potentially leading to arbitrary code execution or a Denial of Service (DoS) via application crash.	5.5	More Details
CVE-2026-44035	Uncontrolled recursion in DcmDicomDir::moveRecordToTree() in dcmdata/libsrc/dcdicdir.cc of OFFIS DCMTK 3.7.0 allows an attacker to cause a denial of service (stack exhaustion and process crash) via a crafted DICOMDIR file with a deeply chained sequence of directory records linked through the Offset of Referenced Lower-Level Directory Entity attribute. Any application that opens the DICOMDIR is affected, including dcmgpd and media viewers built on DCMTK. The issue is fixed in commit ca761f7f3dcaaddaa95be87cf5d736138d7c3a9f.	5.5	More Details

CVE-2026-107730	SumatraPDF is a multi-format reader for Windows. In 3.7.0.22298, LitParseHeader() in src/LitDoc.cpp computes the attacker-controlled <code>hdrLen + nPieces * 16</code> section offset using signed 32-bit arithmetic without validating the complete result. When the component values make that aggregate calculation overflow to a negative value, pointer construction reaches an invalid read in <code>LitU32()</code> , causing deterministic application termination. The supplied evidence does not demonstrate code execution, information disclosure, arbitrary read, or integrity impact. No fixed version is available as of this review.	5.5	More Details
CVE-2026-107211	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.8.1 to 2.11.0, separately parsed pivot-table field indices are used to index the pivot-cache field-name slice without bounds checks. <code>extractPivotTableFields</code> uses <code>getPivotCacheFieldsName</code> output while processing <code>GetPivotTables</code> and trusts the <code>dataField fld</code> attribute as an index. When a crafted workbook supplies a pivot-field count mismatch or an out-of-range <code>dataField fld</code> value before <code>GetPivotTables</code> is called, the unchecked index causes a Go slice-bounds panic that escapes the library, allowing an attacker to crash the process or request worker. No fixed version is available as of this review.	5.5	More Details
CVE-2026-66085	In <code>modem</code> , there is a possible information disclosure due to missing filtering of sensitive data in crash dumps. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2026-108573	A vulnerability was detected in Open Asset Import Library Assimp up to 6.0.5. Affected by this vulnerability is the function <code>IOStreamBuffer::getNextBlock</code> of the component PLY File Handler. Performing a manipulation results in out-of-bounds read. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2026-19737	<code>i2s_esp32_trigger_check()</code> in <code>drivers/i2s/i2s_esp32.c</code> validates the requested direction only for <code>I2S_DIR_BOTH</code> . The <code>I2S_DIR_RX</code> and <code>I2S_DIR_TX</code> branches read <code>dev_cfg->rx.data->configured / dev_cfg->tx.data->configured</code> without first checking the stream pointers. The device instantiation macro <code>I2S_ESP32_STREAM_INIT()</code> sets both <code>.conf</code> and <code>.data</code> to <code>NULL</code> for a direction the devicetree does not describe, so on an instance that wires only one direction — the normal shape for audio output or a worldsemi,ws2812-i2s LED strip — the other direction dereferences a <code>NULL</code> pointer instead of returning an error. <code>i2s_trigger()</code> is a Zephyr syscall, and <code>z_vrfy_i2s_trigger()</code> in <code>drivers/i2s/i2s_handlers.c</code> validates only the device object and the presence of the trigger API pointer; the <code>dir</code> argument is passed to the driver unvalidated. On a build with <code>CONFIG_USERSPACE</code> enabled, a user-mode thread that has been granted the I2S device can issue a single <code>i2s_trigger()</code> call naming the unwired direction and cause a load from address 0 in kernel mode. Among the Espressif parts that carry this driver, userspace is available in-tree only on RISC-V SoCs with <code>CONFIG_RISCV_PMP</code> , and v4.4.0 is the first release where that is buildable: the ESP32-C6 HPCORE selects <code>RISCV_PMP</code> when it is not built for MCUBoot. ESP32-C5 in v4.4.x carries the same PMP-region and userspace linker support but does not select <code>RISCV_PMP</code> by default. Espressif Xtensa targets do not support Zephyr userspace, and in a non-userspace build the bad direction can only come from in-kernel application code. The impact is limited to availability: the access is a read at offset 0 of the missing stream structure, so there is no attacker-controlled offset, no write primitive and no information disclosure. With the default fatal-error handler the resulting exception halts the system, giving an unprivileged user-mode thread a system-wide denial of service. The fix adds the same pointer check the <code>I2S_DIR_BOTH</code> branch already performed and returns <code>-ENOSYS</code> for a direction the instance does not implement; the driver's other entry points (<code>i2s_esp32_config_check()</code> , <code>i2s_esp32_config_get()</code> , <code>i2s_esp32_read()</code> , <code>i2s_esp32_write()</code>) already guarded the pointers, and a static audit found no equivalent unguarded path. The driver defect is older than the affected range. The unguarded dereference is present from v4.2.0 (reached through <code>i2s_esp32_trigger_stream()</code> , whose <code>if (stream)</code> guard tests the address of a struct member and is never false) and takes its present <code>i2s_esp32_trigger_check()</code> form in v4.3.0. No in-tree Espressif configuration before v4.4.0 can run a user-mode thread, so in v4.2.x and v4.3.x the direction argument can only come from trusted kernel code. Those releases carry the bug but are not listed as affected; the fix has also been merged to v4.3-branch as hardening.	5.5	More Details
CVE-2026-80048	A flaw was found in <code>`sssd-kcm`</code> . A local user or process able to connect to the <code>`sssd-kcm`</code> UNIX socket can exploit this vulnerability. By sending a large request length header and then stalling the connection, an attacker can cause the system to preallocate significant memory. This leads to memory exhaustion within the <code>`sssd-kcm`</code> responder, resulting in a Denial of Service (DoS) for affected deployments.	5.5	More Details
CVE-2026-107729	SumatraPDF is a multi-format reader for Windows. In 3.7.0.22298, <code>src/MobiDoc.cpp</code> narrows the untrusted unsigned <code>mobiHdr.hdrLen</code> field to a signed integer for validation; values above <code>INT_MAX</code> become negative and bypass the upper-bound check. When the <code>EXTH</code> flag is set, the original unsigned value is reused as a pointer offset, causing <code>DecodeExthHeader()</code> to read beyond the record buffer. Opening a crafted MOBI file can reliably terminate the application with a native access violation; no code execution, information disclosure, or integrity impact has been demonstrated. No fixed version is available as of this review.	5.5	More Details
CVE-2026-108063	A flaw was found in <code>libhangul</code> . When parsing Hanja dictionary files, the library fails to verify that an entry contains a valid value alongside its key. By providing a specially crafted dictionary file to an application that queries it, an attacker can trigger an unexpected application crash, resulting in a Denial of Service (DoS).	5.5	More Details
CVE-2026-	GenOffice through 0.11.505 contains an incorrect permissions vulnerability in its HTTP MCP server file store that allows local unprivileged users to read uploaded and generated documents. Attackers can list the world-readable <code>genoffice-mcp-http</code> directory under the system temporary directory to read client uploads and	5.5	More Details

108582	converted outputs, bypassing the HTTP bearer token.		
CVE-2026-46571	In NTFS-3G before 2026.7.7, a out-of-bounds read exists in ntfs_fix_file_name() in libntfs-3g/reparse.c that allows an attacker to read possibly confidential information in ntfs-3g process memory by crafting a malicious NTFS image. The out-of-bounds read is triggered by a readlink on a corrupted file.	5.5	More Details
CVE-2026-108858	Predibase LoRAX through 0.12.1 contains a sensitive information exposure vulnerability that writes the caller-supplied api_token from POST /generate request bodies into router logs. Attackers with access to router logs or OTLP trace backends can recover other users' private-adapter tokens recorded through the instrumented GenerateParameters span field.	5.5	More Details
CVE-2026-107889	A flaw was found in the login theme rendering component of Keycloak. The issue occurs because the security filter responsible for cleaning user input can be bypassed, allowing a realm administrator to store malicious scripts in display fields. This could result in unauthorized JavaScript execution in the browsers of users visiting the login page, potentially leading to data exposure or session interference.	5.5	More Details
CVE-2026-88514	An issue in iTerm2 macOS before 3.6.12 allows a local attacker to obtain sensitive information.	5.5	More Details
CVE-2026-87765	In the kernel apsys DVFS driver, there is a possible out-of-bounds read or hardware register corruption due to improper input validation of the frequency index. This could lead to system instability or denial of service with local privileges.	5.5	More Details
CVE-2026-107213	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.9.0 to 2.11.0, GetSlicers checks for ExtLst but dereferences ws.Drawing without checking whether the independently optional drawing element exists. File.GetSlicers reads ws.Drawing.RID after seeing a worksheet extLst element even when the independently optional worksheet drawing element is absent. When a crafted worksheet contains an extLst element without a drawing element and the application calls GetSlicers, the nil ws.Drawing pointer is dereferenced while resolving the drawing relationship, allowing an attacker to panic and terminate an unprotected process. No fixed version is available as of this review.	5.5	More Details
CVE-2026-108789	A vulnerability was identified in deepseek-ai deepseek-harness up to 0.1.1-rc.2. This affects the function agent of the component dsh-workflow-worker-thread. The manipulation leads to enforcement of behavioral workflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2026-44033	Uncontrolled recursion in XMLNode::ParseXMLElement() and XMLNode::emptyTheNode() in the bundled XML parser (ofstd/libsrc/ofxml.cc) of OFFIS DCMTK 3.7.0 allows an attacker to cause a denial of service (stack exhaustion and process crash) via a crafted XML document with deeply nested elements. The parser is reachable through dcmencap when encapsulating a CDA document, and through any application that calls OFXMLParser::parseFile() or OFXMLParser::parseString() on untrusted input. The issue is fixed in commit d12e350e687530eb41e2b0c860aff4d8c04e5941.	5.5	More Details
CVE-2026-108093	A flaw was found in GIMP. The XCF loader processes image-simulation-intent and image-simulation-bpc parasites without ensuring the parasite data is present before dereferencing it. Opening a specially crafted XCF file with a zero-size simulation parasite can cause a NULL pointer dereference and crash the GIMP application.	5.5	More Details
CVE-2026-107608	Improper link resolution before file access in the asset bundling output handling in AWS aws-cdk-lib before 2.267.0 might allow a context-dependent actor to cause files from the build host to be published as the deployed asset. To remediate this issue, users should upgrade to version 2.267.0 or later.	5.5	More Details
CVE-2026-108854	Wanwu before 0.6.3 contains an insecure direct object reference vulnerability that allows any authenticated enabled user to delete other users' legacy AppKeys by supplying a numeric apid. Attackers can iterate sequential key IDs against DELETE /v1/appspace/app/key to revoke AppKeys across organizations, breaking MCP and OpenAPI clients until owners issue new keys.	5.4	More Details
CVE-2026-108619	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to delete message templates via the DELETE /sys/message/sysMessageTemplate/deleteBatch endpoint. Attackers can supply comma-separated template ids from the unguarded list endpoint to delete all sys_sms_template rows, breaking template-based notifications such as workflow reminders.	5.4	More Details
CVE-2026-108616	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragExtDataController deleteBatch handler that allows any authenticated user to delete AI evaluator records. Low-privileged attackers can send comma-separated ids to DELETE /airag/extData/deleteBatch, which lacks owner or tenant checks, deleting other users' evaluator and test-tracking records.	5.4	More Details
CVE-2026-108620	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysPositionController deleteBatch handler that allows any authenticated user to delete organizational positions. Low-privileged attackers can send comma-separated position ids, obtained from the unguarded list endpoint, to remove all	5.4	More Details

	sys_position rows and orphan user-position assignments.		
CVE-2026-107854	Jexactyl is a customisable game management panel and billing system. From 4.0.0 until 4.0.5, the POST /api/client/billing/free/process endpoint accepts a client-controlled server_id and loads the server without restricting the lookup to servers owned by the authenticated account. On installations with billing enabled, an authenticated user can renew or unsuspend another tenant's billable server when its renewal_date is non-null and more than seven days away, even without a subuser relationship to that server. This issue is fixed in version 4.0.5.	5.4	More Details
CVE-2026-108622	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysLogController delete handler that allows any authenticated user to delete audit log entries. Low-privileged attackers can obtain log ids from the unguarded /sys/log/list endpoint and delete chosen sys_log records to erase traces of their actions.	5.4	More Details
CVE-2026-108756	Abilityai Trinity through 0.9.5 contains a missing authorization vulnerability in the Telegram router that allows agent-scoped MCP API keys to perform human-only binding operations. Attackers controlling an agent, typically via prompt injection, can send messages through the owner's bot token, replace the binding with their own token, or delete it.	5.4	More Details
CVE-2026-108644	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysCategoryController delete handler that allows any authenticated user to delete category dictionary nodes. Low-privileged attackers can obtain node ids from the unguarded rootList and childList endpoints and delete entire sys_category subtrees, breaking dependent forms and dictionary fields.	5.4	More Details
CVE-2026-108731	Raven 2.0.0 through 3.0.0 contains a missing authorization vulnerability that allows authenticated users to join invite-only Public workspaces by ignoring the can_only_join_via_invite setting. Attackers with the Raven User role can call the join_workspace method to become persistent members, reading and posting in Public and Open channels.	5.4	More Details
CVE-2026-108586	1MCP Agent (@1mcp/agent) 0.20.0 through 0.39.0 contains an incorrect authorization vulnerability that allows authenticated clients to bypass OAuth tag-scope enforcement using negated advanced tag-filter expressions. Attackers holding a single-tag token can send a filter like not <granted-tag> to list and invoke tools on backend MCP servers outside their granted scopes.	5.4	More Details
CVE-2026-107434	Subscriber Bypass Vulnerability in MicroPayments <= 3.2.9 versions.	5.4	More Details
CVE-2026-108689	Wukong AICRM through 20260610 contains a missing authorization vulnerability that allows authenticated users to write into other users' AI chat sessions by supplying an arbitrary sessionId to POST /chat/send. Attackers can append messages to a victim's conversation and receive streamed assistant replies built from the victim's last 20 messages, disclosing conversation content.	5.4	More Details
CVE-2026-45161	wger is a free, open-source workout and fitness manager. Prior to version 2.6, the `trainer_login` view in wger accepts GET requests and executes `django_login()` without any CSRF protection, because Django's `CsrfViewMiddleware` only enforces tokens on unsafe methods (POST/PUT/PATCH/DELETE). An attacker can embed a single `<img>` tag on a malicious page; when an authenticated trainer loads that page, their browser auto-issues the GET with the session cookie, forcibly rebinding the trainer's session to an arbitrary user account. Version 2.6 fixes the issue.	5.4	More Details
CVE-2026-108691	mall4j through 4.0 contains an improper authorization vulnerability that allows authenticated storefront customers to delete other shoppers' cart items through an operator precedence error in the cleanExpiryProdList SQL statement. Attackers can send one DELETE request to /p/shopCart/cleanExpiryProdList to remove every user's cart entries for off-shelf products, which do not return when products are restocked.	5.4	More Details
CVE-2026-15178	The Fluent Forms plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.2.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Custom-level access and above, to read private form submissions, change submission statuses, permanently delete submissions, and modify global plugin settings.	5.4	More Details
CVE-2026-107445	A flaw was found in Katello where the Flatpak Remote Repositories API does not properly enforce authorization when accessing a flatpak remote repository by identifier. An authenticated user with permission to view flatpak remotes in one organization may be able to access flatpak remote repository information belonging to another organization. The same unscoped lookup is used by the mirror action, which may allow creating a repository in a product the user can edit that is configured with another organization's flatpak remote URL and stored remote credentials.	5.4	More Details
CVE-2026-108585	argocd-mcp (Argo CD MCP Server) through 0.9.0 contains a path traversal vulnerability in the delete_application tool that allows MCP clients to reach unintended API endpoints via unvalidated applicationName values. Attackers or prompt-injected models can supply dot-segment values like ../repositories/ to send authenticated DELETE requests deleting repositories, clusters, or projects within the	5.4	More Details

	token's RBAC permissions.		
CVE-2026-105820	Vault's ACL policy cache allowed namespace traversal when policy names contained path traversal constructs. This may allow a token assigned specially crafted policy names to use the capabilities of policies defined in other namespaces, including the root namespace. This vulnerability (CVE-2026-105820) is fixed in Vault Enterprise 2.1.2, 1.21.12, 1.20.17, and 1.19.23. Vault Community Edition does not support namespaces, and is not affected.	5.4	More Details
CVE-2026-108703	CordysCRM through 1.9.3 contains a missing authorization vulnerability in POST /approval-resource/push that allows authenticated users to submit any resource for approval without ownership checks. Low-privileged attackers can supply arbitrary resourceId values for contracts, invoices, quotations or orders to alter their approval status and read approval details.	5.4	More Details
CVE-2026-102291	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 6.3.1 This is due to the plugin substituting a user's `display_name` into the composed page markup unfiltered and then running the whole result through `do_shortcode()` in `TheFrontend::replace_content()`. Because `display_name` is writable by any user on their own account through the core profile form, this makes it possible for authenticated attackers with Subscriber-level access and above to execute arbitrary shortcodes. Where the page is a users collection — an ordinary team or member-directory page — the shortcode runs in the request of every visitor, including unauthenticated ones. Requires a published page with a Kirki element whose dynamic content is bound to the `display_name` user field.	5.4	More Details
CVE-2026-107450	In Stump through 0.1.10, the updateSmartList and deleteSmartList GraphQL mutations (crates/graphql/src/mutation/smart_lists.rs) depend only on the shared AccessSmartList permission and resolve the target list at Reader access (lacking a creator check). Any authenticated user with that permission can overwrite, delete, or take over another user's smart list. (updateSmartList sets creatorId to the caller identity, and can set visibility to PRIVATE, locking out the original owner.) NOTE: this is unrelated to the graphql crate on crates.io.	5.4	More Details
CVE-2026-106139	In Progress® Kendo UI for Vue (@progress/kendo-vue-charts) starting with version 2.5.0 and prior to 16.2.0, the default Chart tooltip renders the formatted point value as raw HTML without encoding, in both the single-point and the shared tooltip. An attacker with low privileges who can influence a string value bound to the chart can supply HTML containing event handlers that execute JavaScript in a user's browser when the user hovers over the affected data point. Successful exploitation can compromise the confidentiality and integrity of data accessible to the affected application.	5.4	More Details
CVE-2026-106138	In Progress® KendoReact (@progress/kendo-react-charts) starting with version 1.1.0 and prior to 16.2.0, the default Chart tooltip renders the formatted point value as raw HTML without encoding, in both the single-point and the shared tooltip. An attacker with low privileges who can influence a string value bound to the chart can supply HTML containing event handlers that execute JavaScript in a user's browser when the user hovers over the affected data point. Successful exploitation can compromise the confidentiality and integrity of data accessible to the affected application.	5.4	More Details
CVE-2026-108639	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to permanently delete data dictionaries via the deletePhysic handler of SysDictController. Low-privileged attackers can send DELETE requests to /sys/dict/deletePhysic/{id} to irreversibly remove active dictionaries and all their items, bypassing the recycle bin.	5.4	More Details
CVE-2026-108606	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiOcrController deleteById handler that allows any authenticated user to delete OCR records. Low-privileged attackers can obtain record ids from the unguarded GET /airag/ocr/list endpoint and repeatedly delete every shared OCR prompt record stored in Redis.	5.4	More Details
CVE-2026-108643	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to delete category dictionary entries via DELETE /sys/category/deleteBatch. Attackers can obtain node ids from the unguarded rootList and childList endpoints and submit them to recursively delete entire sys_category subtrees, breaking dependent forms and dictionary fields.	5.4	More Details
CVE-2026-108668	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragPromptsController deleteRecycleBin handler that allows any authenticated user to purge AI prompt templates. Low-privileged attackers can send DELETE requests with prompt template ids to permanently remove recycle-bin templates belonging to administrators or other users.	5.4	More Details
CVE-2026-108631	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysDepartPermissionController delete handler that allows low-privileged authenticated users to delete department permission bindings. Attackers can obtain row ids from the unguarded list endpoint and send DELETE requests with the id parameter to remove menus or buttons departments can grant their roles.	5.4	More Details
CVE-2026-	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the deleteBatch handler of AiragPromptsController that allows any authenticated user to delete AI prompt templates. Low-privileged attackers can obtain prompt ids from the unguarded list endpoint and pass them to deleteBatch to remove	5.4	More Details

108666	templates created by administrators or other users.		
CVE-2026-108611	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AigcWordTemplateController delete handler that allows any authenticated user to delete word templates. Low-privileged attackers can send DELETE requests to /airag/word/delete with an id parameter to permanently remove any template from the shared library.	5.4	More Details
CVE-2026-107321	The W3 Total Cache WordPress plugin before 2.10.6 does not confine a media-import file copy to the document root, nor enforce an effective file-type restriction on it, allowing users with the Author role or higher to plant content that, once an administrator runs the import, copies an arbitrary server-readable file into a publicly served directory, exposing it to unauthenticated retrieval.	5.4	More Details
CVE-2026-17538	The LatePoint - Appointment Booking & Reservation plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 5.6.9. This is due to the process_step_customer() function using is_user_logged_in() as the sole gate before merging POSTed customer data into an existing LatePoint customer, without any ownership checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the personal information (first name, last name, email, phone, notes) of arbitrary LatePoint customers, and, when the contact_merge setting is 'phone', to overwrite the victim's email address and take over the account via a password reset.	5.4	More Details
CVE-2026-103482	The Simple Newsletter Plugin - Noptin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noptin_fields[<custom_field_merge_tag>]' (e.g. first_name) parameter in all versions up to, and including, 4.3.10 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. The attack chain requires a published campaign post whose body contains a [[subscriber.*]] merge tag; the unauthenticated attacker first POSTs the entity-encoded payload to the public manage_preferences form (which issues its own nonce on the same page), then pivots execution by embedding their confirm_key in a campaign preview URL sent to a privileged user via social engineering.	5.4	More Details
CVE-2026-108612	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AigcWordTemplateController deleteBatch handler that allows low-privileged authenticated users to delete word templates. Attackers can send a DELETE request to /airag/word/deleteBatch with comma-separated ids to permanently delete any templates in the shared library.	5.4	More Details
CVE-2026-5727	The Hello Plus plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.7.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Contributor-level access and above, to publish their own Hello+ header/footer templates and draft currently active templates owned by higher-privileged users.	5.4	More Details
CVE-2026-108662	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to remove users from tenant product packs via PUT /sys/tenant/deleteTenantPackUser. Attackers can supply arbitrary userId and packId values in the request body to remove any user from any tenant's product pack, revoking permissions such as tenant administrator access.	5.4	More Details
CVE-2026-108613	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragAppController release handler that allows any authenticated user to publish or unpublish other users' AI applications. Low-privileged attackers can send POST requests to /airag/app/release to obtain share tokens exposing applications to anonymous chat access, or invalidate existing share links.	5.4	More Details
CVE-2026-103424	The Anti-Spam by CleanTalk - Spam Protection Without CAPTCHA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 6.88 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. This vulnerability is exploitable once a comment from the attacker's email address has been approved; on default WordPress installations, only the first comment from a given email address is held for moderation, meaning subsequent comments auto-approve and immediately expose the payload to site visitors.	5.4	More Details
CVE-2026-108725	Cheshire Cat AI core through 2.0.23 contains a stored cross-site scripting vulnerability in the uploads plugin that allows authenticated users to upload HTML files via POST /uploads without type restrictions. Attackers can send the public GET /uploads/{path} URL to a signed-in victim, executing script in the application origin with the victim's access_token cookie, including administrators.	5.4	More Details
CVE-2026-108615	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragExtDataController delete handler that allows low-privileged authenticated users to delete AI evaluator records. Attackers can send DELETE requests to /airag/extData/delete with any id parameter to remove other users' AI evaluator or test-tracking records without owner or tenant checks.	5.4	More Details
	The Academy LMS - AI Course Builder, Quizzes, Certificates & eLearning plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.0.3. This is due to the `add_child()` function calling `add_role('academy_student')` on any existing account resolved from the attacker-supplied `email` parameter before `Store::link()` validates the guardian-ward relationship, and failing to roll back that role		

CVE-2026-104022	write when `Store::link()` returns a `WP_Error`. This makes it possible for authenticated attackers with the `academy_guardian` role or higher to elevate any existing WordPress account — including their own — to the `academy_student` role, gaining `edit_posts` (Contributor-equivalent) capabilities and, when the student file-upload setting is enabled, `upload_files` (Author-equivalent) capabilities not granted to the guardian role. When a guardian supplies their own email address, `email_exists()` resolves to their own user ID, causing `Store::link()` to reject the self-link, but because the `add_role()` call has already executed and is never reversed, the academy_student role grant on their own account persists permanently.	5.4	More Details
CVE-2026-108634	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to delete department permission bindings via the DELETE /sys/sysDepartPermission/deleteBatch endpoint. Attackers can obtain row ids from the unguarded list endpoint and submit them in the ids parameter to remove menus and buttons departments can grant to their roles.	5.4	More Details
CVE-2026-108624	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysMessageController deleteBatch handler that allows low-privileged authenticated users to delete message records. Attackers can obtain record ids from the unguarded list endpoint and submit them to deleteBatch to remove any message push records, including pending queued messages.	5.4	More Details
CVE-2026-107698	FFmpeg before 7.1.4 and 8.0.x before 8.0.2 contains a server-side request forgery vulnerability in ff_rtsp_connect() in libavformat/rtsp.c that follows RTSP 3xx redirects without validating the Location URL. Malicious RTSP servers can redirect FFmpeg to internal hosts and ports under other schemes, bypassing -protocol_whitelist, to probe internal network services.	5.4	More Details
CVE-2026-107334	Malcolm's nginx Lua role-based access control (RBAC) layer decides whether an authenticated user may reach a role-restricted path (e.g. /htadmin, /auth, /admin_login, /arkime/api/esadmin, NetBox, upload endpoints) by pattern-matching the raw, percent-encoded request URI. Nginx itself, however, selects which location block actually serves the request using the percent-decoded, normalized URI. Because the RBAC check never percent-decodes its input, an authenticated low-privilege user can request an admin-only path using percent-encoding (e.g. /%68tadmin.php) and have nginx route it to the restricted location while the Lua RBAC gate evaluating the un-decoded raw string finds no matching restriction and grants access.	5.4	More Details
CVE-2026-108682	A weakness has been identified in zhayujie CowAgent up to 2.1.6. The affected element is the function read of the file /upload of the component Web Console. This manipulation causes denial of service. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-107432	Missing Authorization vulnerability in NOUS Ouvert Utile et Simple Event post event-post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event post: from n/a through 6.1.1.	5.4	More Details
CVE-2026-107430	Missing Authorization vulnerability in VideoWhisper.com VideoWhisper Site Manager for ChatGPT, Claude, Codex videowhisper-site-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VideoWhisper Site Manager for ChatGPT, Claude, Codex: from n/a through 1.2.10.	5.4	More Details
CVE-2026-103356	Missing Authorization vulnerability in VillaTheme TMDS tmlds-dropshipping-for-temu-and-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TMDS: from n/a through 1.0.15.	5.4	More Details
CVE-2026-108870	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysRoleController saveDatarule handler that allows low-privileged authenticated users to modify role data rules. Attackers can send permissionId, roleId and dataRuleIds to overwrite data_rule_ids, clearing row-level filters to widen readable records or altering filtering for other roles.	5.4	More Details
CVE-2026-108871	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the saveDatarule handler of SysDepartRoleController that lets low-privileged authenticated users modify department role data rules. Attackers can send crafted permissionId, roleId and dataRuleIds values to overwrite data_rule_ids, widening row-level data access or altering filtering for other department roles.	5.4	More Details
CVE-2026-48211	An authenticated administrator can be induced to delete administrative Import/Export templates through a Cross-Site Request Forgery (CSRF) attack. The OTRS AdminImportExport::TemplateDelete action does not validate the request's ChallengeToken, allowing an unauthenticated remote attacker to craft a malicious request that is executed with the privileges of an active administrator session. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	5.4	More Details
CVE-2026-107203	An incorrect authorization flaw has been found in network interface handling in the Foreman package. The domain and subnet interface API checks only that the caller holds a host permission. It does not apply the search limit on that permission, so the request is answered from every interface on the domain or subnet. A low-privileged network attacker or user must already be allowed to view some hosts and to view a domain or subnet shared with other hosts. They can request that domain or subnet's interfaces. The response	5.4	More Details

	includes interface records of hosts they are not allowed to view. If the attacker or user is also allowed to edit some hosts, they can submit a change to one of those interfaces. The interface is then saved with that change.		
CVE-2026-107380	savg-sanitizer is a PHP SVG/XML sanitizer. Prior to 1.0.0, svg-sanitizer's isHrefSafeValue() validates an SVG href after XML DTD entity expansion, but saveXML() serializes the original entity reference after removing the DTD declaration. A crafted entity such as Tab can appear to the sanitizer as a safe fragment prefix while HTML5 Named Character Reference resolution during inline HTML rendering later converts the surviving reference to whitespace, exposing a javascript: URL. When an application embeds the sanitized SVG inline, a user who activates the link can cause script to execute in the embedding page's origin. This issue is fixed in version 1.0.0.	5.4	More Details
CVE-2026-108877	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in AiragPromptsController that allows any authenticated user to delete AI prompt templates by calling DELETE /airag/prompts/delete. Low-privileged attackers can obtain template ids from the unguarded GET /airag/prompts/list endpoint and logically delete any user's prompt template, making it unavailable to all users.	5.4	More Details
CVE-2026-108112	ruoyi-ai 3.0.0 through 3.1.0 contains a missing authorization vulnerability that allows authenticated users to delete other users' workflows via POST /workflow/del/{uuid}. Attackers can obtain workflow UUIDs from GET /workflow/search and supply them because softDelete() skips the PrivilegeUtil.checkAndGetByUuid() ownership check, removing owners' workflows.	5.4	More Details
CVE-2026-93684	An SQL user using Impala up to and including version 4.5.2 with only SELECT permission can put JavaScript in a table alias and make it run in another user's browser when that user opens the query plan in Impala's Web UI. This is stored XSS (CWE-79). Users are recommended to upgrade to version 4.5.3.	5.4	More Details
CVE-2026-107419	Missing Authorization vulnerability in Cool Plugins AI Translation for Polylang automatic-translations-for-polylang allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Translation for Polylang: from n/a through 1.6.2.	5.4	More Details
CVE-2026-62041	Missing Authorization vulnerability in Ashok Dudhat WP Event Manager wp-event-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Event Manager: from n/a through 3.4.1.	5.4	More Details
CVE-2026-108882	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysPositionController removeUserPosition handler that allows any authenticated user to remove position members. Low-privileged attackers can send DELETE requests with arbitrary userIds and positionId values to delete sys_user_position rows, detaching users from positions without logging.	5.4	More Details
CVE-2026-108884	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysMessageTemplateController delete handler that allows any authenticated user to delete message templates. Low-privileged attackers can obtain template ids from the unguarded list endpoint and delete shipped notification templates, causing system notices and workflow reminders to fail.	5.4	More Details
CVE-2026-13258	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 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-2026-106601	Authentication Bypass Using an Alternate Path or Channel vulnerability in Automattic Jetpack jetpack allows Password Recovery Exploitation.This issue affects Jetpack: from n/a through 16.2.	5.4	More Details
CVE-2026-62028	Missing Authorization vulnerability in bPlugins Before After Image Comparison - Image comparison for WP before-after-image-compare allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Before After Image Comparison - Image comparison for WP: from n/a through 1.1.21.	5.4	More Details
CVE-2026-108885	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysMessageController delete handler that allows low-privileged authenticated users to delete message records. Attackers can send DELETE requests with arbitrary id values to remove any sys_sms row, erasing records of sent notifications without ownership checks.	5.4	More Details
CVE-2026-86833	The MetForm WordPress plugin before 4.3.1 does not sanitize or escape submitted form-field values before inserting them into the HTML body of its email notifications, allowing unauthenticated attackers to inject arbitrary markup into the administrator and submitter notification emails the site sends.	5.4	More Details
CVE-2026-	OTRS does not sufficiently enforce the uniqueness of customer user identities across multiple configured CustomerUser backends. When multiple backends, such as a database and LDAP, are configured, the uniqueness check for customer user email addresses is performed only within the selected backend. As a result, an authenticated user with permission to create or modify customer users may create a customer user whose email address is already assigned to a customer user in another backend. This can result in multiple customer user records representing the same communication identity. Depending on the affected workflow and backend resolution, customer-related information or email communication may subsequently be	5.4	More Details

78359	associated with or exposed to the wrong customer user. The vulnerability does not allow unauthenticated users to create customer accounts. Exploitation requires permissions to create or modify customer users. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected		
CVE-2016-20098	Moderator Toolbox (reddit-moderator-toolbox) before 4.0.14 contains a stored cross-site scripting vulnerability in the removalreasons module, which inserts subreddit toolbox wiki fields into popup HTML without encoding. Attackers who can edit the toolbox wiki page can plant JavaScript in fields like pmsubject, header, or reason titles to act with moderators' Reddit sessions.	5.4	More Details
CVE-2026-108825	A vulnerability has been found in yangzongzhuan RuoYi up to 4.8.3. This affects the function checkRoleAllowed of the file /system/role/authDataScope. Such manipulation of the argument roleKey leads to improper privilege management. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-78407	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 are 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-2026-107798	jivejdon from commit 595d8d22 through commit ee67a65e contains a stored cross-site scripting vulnerability in the default-enabled TextStyle filter that inserts unvalidated URLs into anchor href attributes. Authenticated attackers can post messages with javascript: links or quote-breaking URLs to execute JavaScript when other users click or hover over rendered links.	5.4	More Details
CVE-2026-107799	Jivejdon through 5.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject script by posting unsanitized forum message bodies. Message bodies are rendered by messageListBody.jsp with filter="false" and non-escaping default filters, executing script in the browser of every user viewing the thread.	5.4	More Details
CVE-2026-107800	Jivejdon through 5.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject script into private short messages because receiveshortmessage.jsp renders unfiltered message bodies. Attackers can send a short message containing script, which ToolsUtil.convertURL() passes through unchanged, to execute code in the recipient's browser when opened.	5.4	More Details
CVE-2026-107801	Jivejdon through 5.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to execute JavaScript by uploading attachments with an attacker-supplied Content-Type. Attackers can upload a file declared as text/html, which UploadShowAction serves inline, and share its link to run JavaScript on the application's origin for viewing users.	5.4	More Details
CVE-2026-105888	Missing Authorization vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through 5.30.0.1.	5.4	More Details
CVE-2026-16830	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a remote authenticated attacker to modify data and cause a denial of service due to an SQL injection vulnerability.	5.4	More Details
CVE-2026-108855	UnicomAI Wanwu through 0.6.5 contains a missing authorization vulnerability that allows any authenticated enabled user to revoke other users' AppKeys for arbitrary apps via the unpublish endpoint. Attackers can supply a target appld and appType from the exploration marketplace to delete other users' api_key rows across organizations, cutting off MCP and OpenAPI client access.	5.4	More Details
CVE-2026-109178	jshERP through 3.6 contains a missing authorization vulnerability in LogController that allows any authenticated user to forge, modify, or delete audit log entries. Low-privilege users can call /log/add, /log/update, /log/delete, and /log/deleteBatch to fabricate entries, rewrite user and IP fields, or erase records to hide activity.	5.4	More Details
CVE-2026-109176	MoguBlog through 6.2 contains an insecure direct object reference vulnerability that allows authenticated administrators to delete other administrators' files via POST /networkDisk/deleteFile and batchDeleteFile. Attackers can supply another administrator's file or folder uid, which NetworkDiskServiceImpl.deleteFile never checks against admin_uid, removing stored objects from local storage, Qiniu or MinIO.	5.4	More Details
CVE-2026-107396	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to 3.3.13, users who can manage events or create content, including speakers who can upload material, can store crafted javascript URLs in fields that accept custom URLs. A user who follows one of these URLs can execute attacker-controlled script in the user's browser in the Indico origin. This issue is fixed in version 3.3.13.	5.4	More Details
CVE-	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in TMT		More

2026-92085	Machinery Industry and Trade Co. Ltd. Talassoft Industrial Management Software allows Stored XSS. This issue affects Talassoft Industrial Management Software: before V16.0.1.	5.4	Details
CVE-2026-92415	— Use of Externally-Controlled Input to Select Classes or Code vulnerability in Apache Jackrabbit's WebDAV/Davex client. A malicious WebDAV/DavEx server, or an attacker able to intercept the connection, can cause the client to instantiate arbitrary classes from its classpath, which can lead to arbitrary file creation or truncation. Only applications that use jackrabbit-spi2dav (directly or through jackrabbit-jcr2dav) to connect to a remote repository are affected. Jackrabbit servers are not affected. Category: unsafe reflection on wire data (HIGH). This issue affects Apache Jackrabbit: from 2.23.0 through 2.23.5, from 2.22.0 through 2.22.4, from 2.20.0 through 2.20.17. Users are recommended to upgrade to versions 2.23.6, 2.22.5, or 2.20.18 which fix the issue.	5.3	More Details
CVE-2026-107830	Jivejdon from commit e0306088 through commit ee67a65e lacks rate limiting on the unauthenticated /account/smsVRAAction endpoint handled by SmsQQAction, allowing unlimited SMS sending. Attackers can load newAccount.jsp to set session attributes, then repeatedly call the endpoint to harass arbitrary phone numbers and exhaust the operator's Tencent Cloud SMS balance.	5.3	More Details
CVE-2026-19585	HashiCorp go-getter versions before 1.8.10 and go-getter/v2 versions before 2.2.5 are vulnerable to path traversal during S3 and GCS directory downloads, which may allow files to be written outside the requested destination. This vulnerability (CVE-2026-19585) is fixed in go-getter 1.8.10 and go-getter/v2 2.2.5.	5.3	More Details
CVE-2026-104074	Coturn 4.10.0 contains an uninitialized memory disclosure vulnerability that allows remote unauthenticated attackers to leak stack memory contents by sending a TURN Allocate request without credentials. Attackers can exploit the stun_init_error_response_common_str() function in src/client/ns_turn_msg.c, which fails to zero-initialize the avalue buffer before computing its length with strlen() and copying leaked stack bytes into the ERROR-CODE reason phrase, exposing pointer fragments that weaken ASLR and enable precise version fingerprinting.	5.3	More Details
CVE-2026-108788	A vulnerability was determined in deepseek-ai deepseek-harness up to 0.1.1-rc.2. The impacted element is the function spawn of the component Sandbox. Executing a manipulation of the argument Profile can lead to sandbox issue. It is possible to launch the attack on the local host. 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-2026-105198	The Appointment Booking Plugin WordPress plugin before 5.7.3 does not verify that the caller owns the order referenced by an order-item identifier before rendering that order's confirmation summary, letting an unauthenticated visitor retrieve any customer's name, contact details and order confirmation code by supplying a sequential order-item id.	5.3	More Details
CVE-2026-66480	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in YITH YITH WooCommerce Product Add-Ons allows Retrieve Embedded Sensitive Data. This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.34.0.	5.3	More Details
CVE-2026-103329	The Super Payments WordPress plugin before 1.43.1 does not properly verify the authenticity of incoming payment webhook notifications, as the signing key used to validate their signature is empty by default, allowing unauthenticated attackers to forge a valid signature and mark arbitrary WooCommerce orders as paid without payment.	5.3	More Details
CVE-2026-86816	The WPCafe WordPress plugin before 3.0.21 does not restrict access to some of its REST API endpoints, allowing unauthenticated attackers to read WooCommerce product data, including per-product sales counts, exact stock levels, and private product meta, that WooCommerce itself keeps behind authentication.	5.3	More Details
CVE-2026-62040	Missing Authorization vulnerability in DEV Institute Restrict User Access – Membership Plugin with Force restrict-user-access allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Restrict User Access – Membership Plugin with Force: from n/a through 2.8.1.	5.3	More Details
CVE-2026-107420	Unauthenticated Bypass Vulnerability in Pay With MetaMask For WooCommerce – Cryptocurrency Payment Gateway <= 1.7.2 versions.	5.3	More Details
CVE-2026-3717	The CV Builder – Professional Resume Builder SaaS plugin for WordPress is vulnerable to unauthorized arbitrary file upload due to a missing capability check on the 'wp_save_signature_image' function in all versions up to, and including, 1.3.1. This makes it possible for unauthenticated attackers to upload arbitrary content to the WordPress uploads directory as png files.	5.3	More Details
CVE-2026-62042	Missing Authorization vulnerability in unFocus Projects Scripts n Styles scripts-n-styles allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Scripts n Styles: from n/a through 3.5.8.	5.3	More Details
CVE-2026-87846	The Shipping for Nova Poshta WordPress plugin through 1.19.8 does not perform any authorisation, nonce or ownership checks on one of its AJAX actions available to unauthenticated users, allowing anyone to delete the shipment records of arbitrary orders and to make the store issue the carrier's waybill-deletion request for those orders using the store's own stored API credentials.	5.3	More Details

CVE-2026-108772	A security vulnerability has been detected in bleenco abstruse up to 2.1.0. This issue affects the function filepath.join of the file server/api/worker/download_cache.go of the component Cache Endpoint. Such manipulation of the argument File leads to path traversal. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-86827	The BackWPup WordPress plugin before 5.7.7 does not verify that a request to its cron-triggered backup execution handler actually originates from WordPress's internal scheduled-event dispatch, allowing unauthenticated attackers to force any existing backup job to run immediately, independent of its configured trigger type or schedule.	5.3	More Details
CVE-2026-107863	Missing Authorization vulnerability in Codecton Products Restricted Users for WooCommerce woo-products-restricted-users allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Products Restricted Users for WooCommerce: from n/a through 0.7.	5.3	More Details
CVE-2026-105322	The Magee Shortcodes WordPress plugin through 2.1.1 does not restrict the recipient of some of its unauthenticated contact-form actions, allowing unauthenticated users to send arbitrary emails to any address through the site (mail relay).	5.3	More Details
CVE-2026-108770	A weakness has been identified in Appwrite up to 2.3.0. This vulnerability affects the function PublicHostname of the file src/Appwrite/Platform/Modules/Avatars/Http/Screenshots/Get.php of the component Browser Screenshot Service. This manipulation of the argument url causes server-side request forgery. The attack can be initiated remotely. Upgrading to version 2.4.0 is able to resolve this issue. Patch name: 393255e7302ae5503331d45802e2eee01c6a47fe. You should upgrade the affected component.	5.3	More Details
CVE-2026-92990	The SendPress Newsletters WordPress plugin through 1.26.1.20 protects a logging endpoint with a hardcoded token that is the same on every site rather than a per-site secret, allowing unauthenticated users to read newsletter sending logs, including recipient email addresses.	5.3	More Details
CVE-2026-108822	A vulnerability was detected in Kamailio up to 6.0.7/6.1.3. The affected element is the function isup_get_calling_party of the file src/modules/sipt/ss7_parser.c of the component sipt Module. The manipulation of the argument length results in buffer overflow. The attack may be performed from remote. Upgrading to version 6.0.8 and 6.1.4 is sufficient to fix this issue. The patch is identified as 3667bebf8d0bea07ed16218fd921d07db87aeb21. Upgrading the affected component is advised.	5.3	More Details
CVE-2026-88931	The Social Web Suite WordPress plugin through 4.1.12 does not restrict which of its settings may be written through an unauthenticated endpoint, allowing attackers to overwrite arbitrary Social Web Suite WordPress plugin through 4.1.12 options, including the shared secret that guards its own privileged endpoints.	5.3	More Details
CVE-2026-94275	The Track Orders for WooCommerce WordPress plugin before 1.2.7 does not verify ownership of an order before returning its billing details, allowing unauthenticated attackers to obtain a customer's name, email address, phone number, postal address and order history by supplying that customer's email address.	5.3	More Details
CVE-2026-94375	The Order Export & Order Import for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.7.8 via the get_file_path. This makes it possible for unauthenticated attackers to extract download exported order CSV files containing customer PII — including names, billing and shipping addresses, email addresses, phone numbers, and order contents — directly over HTTP with no authentication. This is exploitable whenever the .htaccess and index.php guard files are absent from wp-content/webtoffee_export/, which can occur after any uninstall/reinstall cycle, migration, backup restore, or staging sync, since the export directory persists but its guard files do not; export filenames follow a fully deterministic second-precision timestamp pattern, making them brute-forceable across any suspected export window.	5.3	More Details
CVE-2026-107585	Uncontrolled eviction in the pending sign-in tables of the REST API in Progressive Robot hMailServer 6.3.4 and 6.3.5 allows a remote unauthenticated attacker to make other users' OpenID Connect, SAML and passkey sign-ins fail. The routes that start a single sign-on and hand out a passkey sign-in challenge are reached without authentication and stored pending state in bounded tables that dropped their oldest entry when full, whoever had started it. An attacker who starts sign-ins a few times a second (about a hundred a second for passkeys) pushes every other user's pending sign-in out of the table before that user's browser returns, denying single sign-on and passkey sign-in for as long as the requests continue.	5.3	More Details
CVE-2026-87841	The UnitechPay WordPress plugin through 1.0.6.3 does not verify the authenticity of the payment notifications it receives, allowing unauthenticated attackers to mark orders placed through it as paid without any payment being made, as well as to force other orders into a failed state.	5.3	More Details
CVE-2026-105876	Missing Authorization vulnerability in WP Chill Modula Image Gallery modula-best-grid-gallery allows Retrieve Embedded Sensitive Data.This issue affects Modula Image Gallery: from n/a through 3.0.11.	5.3	More Details
CVE-2026-108578	A vulnerability was identified in Neterbit NW-431F 20250715. Impacted is an unknown function of the file /sms.json of the component Embedded Web Server. Such manipulation leads to information disclosure. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond	5.3	More Details

	in any way.		
CVE-2026-85479	The STTP-based data publisher on openPDC accepts network connections without authentication in its default configuration. An unauthenticated network attacker can connect to this interface and exchange data with it.	5.3	More Details
CVE-2026-18496	The Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 11.4.3 via the <code>wpbcb_is_show_popover_in_flex_timeline()</code> function. This makes it possible for unauthenticated attackers to extract sensitive data including names, email addresses, and phone numbers of customers who have made bookings.	5.3	More Details
CVE-2026-108596	OpenLIT 2.1.0 contains an authorization bypass vulnerability that allows authenticated users to read other projects' telemetry by supplying a forged <code>x-openlit-project-id</code> header. Attackers who know a victim project id and database config id can query the trace read API to obtain traces including LLM prompts and completions.	5.3	More Details
CVE-2026-107293	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 0.3.4 until 1.107.4 and 2.27.1, OpenTelemetry instrumentation configured with <code>InstrumentationSettings(include_content=False)</code> can export retry prompts outside tool calls in <code>gen_ai.input.messages</code> and <code>pydantic_ai.all.messages</code> . Agents using <code>NativeOutput</code> , <code>PromptedOutput</code> , or output validators on text output can therefore disclose validation feedback, including invalid model values quoted by that feedback, to readers of the telemetry backend. Tool-call retries and deployments that do not use <code>include_content=False</code> are not affected by this specific path. This issue is fixed in versions 1.107.4 and 2.27.1.	5.3	More Details
CVE-2026-107298	<code>msgpack5</code> is a <code>msgpack</code> v5 implementation for <code>node.js</code> and the browser. Prior to 6.1.0, the array and map decoding paths have no nesting-depth limit, allowing an attacker who can provide <code>MessagePack</code> input to submit deeply nested containers that exhaust the JavaScript call stack and interrupt a process, worker, or request handler. This issue is fixed in version 6.1.0.	5.3	More Details
CVE-2026-106563	Backstage is an open framework for building developer portals. Prior to 0.21.8, the <code>@backstage/plugin-kubernetes-backend</code> package is affected by improper entity validation in deprecated <code>kubernetes</code> services endpoint. An authenticated user with <code>Kubernetes</code> read permissions could access <code>Kubernetes</code> workload data beyond their intended scope by supplying crafted entity data to the deprecated services endpoint. The exposure is limited to read-only access to <code>Kubernetes</code> object metadata across configured clusters. This issue is fixed in version 0.21.8.	5.3	More Details
CVE-2026-108810	A security flaw has been discovered in <code>tsi-coop tsi-dpdp-cms</code> 0.5.0/0.5.1/0.5.2. Impacted is an unknown function of the component <code>JSON Schema Validation</code> . The manipulation of the argument <code>_func</code> results in information disclosure. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.5.3 is recommended to address 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.	5.3	More Details
CVE-2026-108554	<code>PDFMathTranslate</code> (<code>pdf2zh</code>) through 1.9.11 contains a server-side request forgery vulnerability that allows unauthenticated attackers to make the server fetch arbitrary URLs via the <code>Link</code> input. The <code>translate_file</code> handler passes user URLs to <code>download_with_limit</code> without scheme or address validation, letting attackers reach internal services and cloud metadata endpoints and retrieve returned PDFs.	5.3	More Details
CVE-2026-76286	In Splunk MCP Server versions below 1.2.1, Splunk MCP Server could send the Splunk platform authentication token of a user who runs a custom Application Programming Interface (API) tool to the URL configured for that tool. If another user controls that URL, they could capture the token and use it to access data and perform actions as the user who ran the tool. Successful exploitation requires a user who holds a role that contains the <code>mcp_tool_execute</code> capability to run a custom API tool configured by another user. For more information see Configure the Splunk MCP Server (https://help.splunk.com/en/splunk-enterprise/mcp-server-for-splunk-platform/1.2/configure-the-splunk-mcp-server) and Managing custom tools in Splunk MCP Server (https://help.splunk.com/en/splunk-enterprise/mcp-server-for-splunk-platform/1.2/managing-custom-tools-in-splunk-mcp-server) in the Splunk documentation.	5.3	More Details
CVE-2026-76281	Improper Access Control. Splunk addressed multiple internally identified vulnerabilities in Splunk Enterprise versions 10.4.3, 10.2.7, 10.0.10, and 9.4.15. The vulnerabilities are grouped by Common Weakness Enumeration (CWE), with one Common Vulnerabilities and Exposures (CVE) identifier assigned to each group. See Details for more information.	5.3	More Details
CVE-2026-107271	Gophish through 0.12.1 contains a rate limit bypass vulnerability that allows unauthenticated attackers to evade <code>/login</code> throttling by spoofing <code>X-Forwarded-For</code> or <code>X-Real-IP</code> headers. Attackers can send a different forwarded address per request so the limiter keyed on rewritten <code>RemoteAddr</code> never triggers, enabling unlimited password guessing and credential stuffing.	5.3	More Details
CVE-2026-107210	<code>ImageMagick</code> is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-30 and 6.9.13-55, a crafted highly compressed <code>MAT</code> image can make the <code>MAT</code> decoder create temporary files larger than the configured security-policy limit, bypassing resource restrictions and consuming excessive disk space. This issue is fixed in versions 7.1.2-30 and 6.9.13-55.	5.3	More Details

CVE-2026-107208	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-30 and 6.9.13-55, a crafted XMP profile can reach a recursion limit that is handled as a fatal condition instead of an ordinary exception, terminating the image-processing process. This issue is fixed in versions 7.1.2-30 and 6.9.13-55.	5.3	More Details
CVE-2026-106605	Improper Validation of Specified Quantity in Input vulnerability in WP Desk Flexible Quantity – Measurement Price Calculator for WooCommerce flexible-quantity-measurement-price-calculator-for-woocommerce allows Input Data Manipulation.This issue affects Flexible Quantity – Measurement Price Calculator for WooCommerce: from n/a through 2.3.22.	5.3	More Details
CVE-2026-107166	A weakness has been identified in Open5GS up to 2.7.7. This vulnerability affects the function ogs_pfcx_xact_local_create of the file src/upf/gtp-path.c of the component GTP-U Receive Path. This manipulation causes allocation of resources. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. Patch name: 9ffc252482d9b03ac01abcedbe95497ff4f95dd0. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2026-108592	mini-swe-agent 1.10.0 through 2.4.6 contains an information exposure vulnerability in BubblewrapEnvironment because bwrap omits --clearenv, so sandboxed commands inherit the host environment. Attackers using prompt injection in processed task content can make the agent read API keys from the environment and exfiltrate them over the shared network.	5.3	More Details
CVE-2026-27434	Missing Authorization vulnerability in sc Internet Vivoo WP Rentals wprentals allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Rentals: from n/a through 3.14.2.	5.3	More Details
CVE-2026-106577	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31 and 6.9.13-56, unescaped or untrimmed values can inject code into output generated by PostScript coders. This issue is fixed in versions 7.1.2-31 and 6.9.13-56.	5.3	More Details
CVE-2026-78356	The OTRS Agent Frontend configuration endpoint can be accessed without authentication. This allows unauthenticated remote users to retrieve internal application configuration that is intended for use by the authenticated Agent Frontend. The exposed information may include configured frontend routes and their associated authorization groups, authentication configuration, enabled product features, third-party integration settings, and other implementation details. The exposed configuration does not directly contain user credentials or provide unauthorized modification of the OTRS configuration. However, the disclosed information may assist an attacker in fingerprinting the affected OTRS installation and identifying enabled functionality or security-relevant configuration that could be used to prepare further attacks. This issue affects OTRS: * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X	5.3	More Details
CVE-2026-106576	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31, a crafted XMP profile can trigger excessive work while the parser determines a rational value's numerator and denominator, causing denial of service. This issue is fixed in version 7.1.2-31.	5.3	More Details
CVE-2026-108950	Open Source Social Network (OSSN) through 10.1 contains a missing authorization vulnerability in ossn_album_page_handler that allows unauthenticated attackers to download files via album/getphoto and album/getcover. Attackers can enumerate sequential file GUIDs to retrieve friends-only album photos and other stored files without any access check.	5.3	More Details
CVE-2026-106575	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31, a crafted Magick script can cause an opened file pointer to remain unclosed, allowing repeated processing to exhaust available file descriptors. This issue is fixed in version 7.1.2-31.	5.3	More Details
CVE-2026-84897	src/internal.c in wolfSSL wolfSSH through 1.5.0 admits the server-to-client Diffie-Hellman group exchange messages SSH_MSG_KEX_DH_GEX_GROUP (31) and SSH_MSG_KEX_DH_GEX_REPLY (33) when a server receives them from an unauthenticated client. IsMessageAllowedServer() applies no direction check to the key exchange message range: when the peer is keying and no particular message is expected, which is the state a server is in for the whole window after it processes the client's KEXINIT because nothing sets handshake->expectMsgId there, the function falls out of its expectation branch without a verdict and reaches a numeric bound that admits every message id from 30 through 34. A client that negotiates diffie-hellman-group-exchange-sha256 and then sends message 31 makes the server run the client-side handler DoKexDhGexGroup(), which validates the attacker-supplied group with two 8-round Miller-Rabin primality tests, one on p and one on (p-1)/2, on a value of up to 8192 bits. The handler then returns success: the server stores the attacker's prime and generator, generates a Diffie-Hellman key pair in the attacker's group, and sends the client-role message SSH_MSG_KEX_DH_GEX_INIT (32) back to the attacker. Published RFC 3526 safe primes are the worst-case input and cost the attacker nothing to obtain. The primality validation was added in 1.5.0; versions from 1.2.0 through 1.4.22 admit the same message and enter the same client-role path without the primality cost. Message 33 is admitted as well, but on a server it is rejected before any cryptography because no public key check callback is registered, so it carries no comparable cost. Builds that define WOLFSSH_NO_DH_GEX_SHA256, which is implied by WOLFSSH_NO_DH or NO_SHA256, are unaffected.	5.3	More Details
CVE-	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to		

2026-106574	7.1.2-31, a client connected to the distributed pixel cache server can send crafted pixel data that triggers an integer-size calculation error and a heap buffer overwrite, crashing the server. This issue is fixed in version 7.1.2-31.	5.3	More Details
CVE-2026-106573	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31 and 6.9.13-56, a missing limit check in the MVG decoder allows a crafted MVG image to trigger an excessively long-running operation. This issue is fixed in versions 7.1.2-31 and 6.9.13-56.	5.3	More Details
CVE-2026-106572	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-30 and 6.9.13-55, a missing recursion-depth check in the CALS decoder allows a crafted CALS image to exhaust the call stack and terminate the process. This issue is fixed in versions 7.1.2-30 and 6.9.13-55.	5.3	More Details
CVE-2026-106569	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32, missing validation and resource checks in the ASE decoder allow a crafted ASE image to cause a crash or a long-running operation. This issue is fixed in version 7.1.2-32.	5.3	More Details
CVE-2026-106568	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32 and 6.9.13-57, a crafted XMP profile embedded in an image can cause the profile parser to enter an infinite loop, preventing image processing from completing. This issue is fixed in versions 7.1.2-32 and 6.9.13-57.	5.3	More Details
CVE-2026-87110	An unauthenticated user with network access to the Ops Manager web port can repeatedly request monitoring endpoints that perform costly work without rate limiting. This can temporarily slow other traffic served by the same process while requests continue.	5.3	More Details
CVE-2026-107315	pgjdbc, the PostgreSQL JDBC Driver, versions 42.7.4 through 42.7.13 pads a value that is shorter than its declared length with bytes left in its send buffer instead of zeros, and the server stores those bytes as part of the value. The bytes are messages the driver sent earlier on the same connection: SQL text and parameter values of recent statements, which on a pooled connection can come from other requests. Each padded value can carry up to 8192 bytes of this traffic, or 16320 bytes on a connection with GSS encryption. The padding happens when an application declares a length larger than the data it supplies, through PreparedStatement.setObject with a ByteStreamWriter, CopyIn.writeToCopy, PGCopyOutputStream.write, LargeObject.write, or Blob.setBytes. The driver accepts these calls without an error. An attacker who can make the application store such a value and read it back can collect earlier traffic. Applications whose declared lengths always match their data are not affected. Versions 42.7.3 and earlier pad with zeros.	5.3	More Details
CVE-2026-106564	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32, a crafted EXR image can cause the EXR decoder to write beyond a heap buffer, causing the process to crash. This issue is fixed in version 7.1.2-32.	5.3	More Details
CVE-2026-108595	Phi 0.3.0 through 0.28.4 contains a permission bypass vulnerability that allows spawned sub-agents to escape workspace_only_writes and readonly mode by supplying an unchecked workdir to agent_spawn. Attackers can plant prompt-injected instructions in processed content so the agent spawns a worker rooted elsewhere, causing unapproved file writes anywhere the user can write.	5.3	More Details
CVE-2026-107218	Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. From 2.10.1 to 2.11.0, RIGHT validates the requested length with UTF-16 code-unit counts but slices a rune array using Unicode code-point counts. RIGHT reaches leftRight through CalcCellValue, where countUTF16String validates one unit but utf8.RuneCountInString supplies the slice index in another. When RIGHT evaluates supplementary-plane text with a requested character count between the rune count and UTF-16 code-unit count, the inconsistent units produce a negative rune-slice index, allowing an attacker to panic during formula evaluation. No fixed version is available as of this review.	5.3	More Details
CVE-2026-87109	An authenticated Ops Manager organization member can retrieve another member's pending authenticator enrollment seed through user-listing endpoints while that member's enrollment is unconfirmed. This results in disclosure of secret authentication material to another member of the same organization or project.	5.3	More Details
CVE-2026-107820	x64dbg-MCP Server is a native Model Context Protocol (MCP) plugin for x64dbg that exposes the debugger's full functionality over HTTP. Prior to 1.2, src/core/mcp_server.zig parses an unbounded Content-Length value in parseContentLength() and uses it in unchecked usize addition in wsRecv() before token authentication. The server listens on 0.0.0.0 by default in affected versions. An unauthenticated network client can supply a near-maximum Content-Length value to trigger a runtime integer-overflow panic in Debug and ReleaseSafe builds, terminating the entire x64dbg process and its live debugging session. The overflowed value is used only in a comparison, so the impact is limited to denial of service rather than memory corruption or code execution. This issue is fixed in version 1.2.	5.3	More Details
CVE-2026-108903	pH7Builder (pH7 Social Dating CMS) before 19.3.0 contains a CAPTCHA bypass vulnerability that allows unauthenticated attackers to skip form validation by supplying a client-chosen form ID to PFBC Form::isValid(). Attackers can load a CAPTCHA-free form like login or search, then submit its ID with contact, comment, forum, invite or signup data to automate abuse.	5.3	More Details
CVE-	Missing Authorization vulnerability in Visual Composer Visual Composer Website Builder visualcomposer		More

2026-106596	allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Visual Composer Website Builder: from n/a through 45.16.3.	5.3	Details
CVE-2026-107575	Inefficient algorithmic complexity in the SPF macro expansion of Progressive Robot hMailServer 6.3.4 and 6.3.5 allows a remote unauthenticated attacker to consume worker-thread time by publishing a crafted SPF record. RFC 7208 section 7.1 requires a name too long to look up to lose whole labels from the left; the server did this by removing one label at a time and copying the rest of the name each time, so the work grew with the square of the expansion. An attacker who publishes an SPF record for a domain they control, with a mechanism whose domain-spec expands through macros to a name far longer than 253 characters, makes the SPF check of a message from that domain take several seconds. The expansion is bounded by SPF's own per-term and per-macro limits, so the loss of availability is partial.	5.3	More Details
CVE-2026-108103	Open5GS through 2.8.0 contains a heap out-of-bounds read vulnerability in ogs_pfcparse_dropped_dl_traffic_threshold() that allows remote unauthenticated attackers to read past IE buffers via short IEs. Attackers can send PFCP Session Establishment or Modification Requests to the UPF on UDP port 8805 with DLPA and DLBY flags set, potentially crashing the UPF.	5.3	More Details
CVE-2026-104724	The FireBox – WooCommerce Popup Builder, Exit Intent Popup, Email Optin & Cart Abandonment plugin for WordPress is vulnerable to generic SQL Injection via FireBox Form Display Condition in all versions up to, and including, 3.1.13 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 author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. On fresh installations of version 3.1.10 and later, exploitation requires administrator-level access; however, on sites upgraded from a version prior to 3.1.10, the preserveCampaignRoleAccess() migration grants the edit_fireboxes capability to any role that previously held edit_posts, reducing the minimum required privilege to Author-level.	5.3	More Details
CVE-2026-107842	Contao is an Open Source CMS. From version 4.0.0 until 5.3.50 and 5.7.12, ModuleSearch can disclose protected page titles, URLs, and indexed context snippets to unauthenticated visitors when contao.search.index_protected is changed from enabled to disabled. Authorization metadata is stored per row in tl_search, but disabling the setting removes the protected-row filter without deleting rows indexed while protection was enabled. The protected pages continue to return an authorization response, so this issue exposes search metadata and indexed text rather than bypassing page access. This issue is fixed in versions 5.3.50 and 5.7.12.	5.3	More Details
CVE-2026-108716	mcp-remote 0.8.0 through 0.14.3 contains a cleartext transmission vulnerability in authorizeWithDeviceCode that sends client secrets and receives tokens without enforcing HTTPS endpoints. When discovered device authorization and token endpoints are non-loopback http URLs, on-path network attackers can capture the client secret plus issued access and refresh tokens.	5.3	More Details
CVE-2026-108721	Open Computer Use through 1.0.0 on macOS contains an improper case sensitivity handling vulnerability that allows local MCP callers to bypass the password-manager denylist using case-variant bundle identifiers. Attackers, including prompt-injected model turns, can pass identifiers like com.1Password.1Password to get_app_state and action tools to read accessibility trees, capture screenshots, and drive unlocked password manager interfaces.	5.3	More Details
CVE-2026-107843	Contao is an Open Source CMS. From version 4.1.0 until 5.3.50 and 5.7.12, ModuleRegistration::compile() enters its follow-up registration branch on any POST to a page containing the registration module without verifying FORM_SUBMIT or the preceding captcha result. resendActivationMail() can then invoke OptInToken::send() without rate limiting, allowing an unauthenticated attacker to cause repeated activation emails to be sent to an address with a pending registration and to determine whether that pending registration exists. The branch is reachable only when reg_activate is enabled and the target has an unconfirmed registration and opt-in token. This issue is fixed in versions 5.3.50 and 5.7.12.	5.3	More Details
CVE-2026-107844	Contao is an Open Source CMS. From version 5.0.0 until 5.3.50 and 5.7.12, ImagesController joins the user-controlled {path} parameter to the configured image target directory with Path::join() but does not use Path::isBasePath() to verify that the canonical path remains inside that directory. An unauthenticated request containing encoded parent-directory segments can therefore return files under the project directory through BinaryFileResponse when their names use an extension allowed by contao.image.valid_extensions. The route can also reveal whether arbitrary paths exist, and debug responses can disclose absolute filesystem paths, but paths below the upload directory were not shown to be readable. This issue is fixed in versions 5.3.50 and 5.7.12.	5.3	More Details
CVE-2026-108755	Hatchet through 0.110.5 contains an allocation of resources without limits vulnerability that allows unauthenticated attackers to exhaust memory via the SNS ingestion endpoint. Attackers can send arbitrarily large or concurrent request bodies to POST /api/v1/sns/{tenant}/{event} with any UUID, which the SnsUpdate handler buffers before signature verification, degrading availability.	5.3	More Details
CVE-	Nginx UI is a web user interface for the Nginx web server. From 2.2.0 until 2.6.0, the bundled reverse proxy does not preserve the external client identity used by Gin because the backend has no trusted proxy configuration. Management requests can be attributed to loopback and pass the IP allowlist loopback		More

2026-107804	exception, although valid credentials are still required. Failed logins from different external clients are also attributed to the same loopback address, allowing an unauthenticated attacker to trigger a shared temporary login ban for password or OTP authentication without invalidating existing sessions. This issue is fixed in version 2.6.0.	5.3	Details
CVE-2026-103365	The Bookly – Online Scheduling and Appointment Booking System plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 28.4 via the classic booking form's Details step. The endpoint bookly_render_details is registered for both wp_ajax and wp_ajax_nopriv, the module overrides csrfTokenValid() to always return true, and Bookly\Frontend\Components\Booking\InfoText::getCodes() calls UserBookingData::getCustomer() to load the persisted Customer entity keyed solely by the attacker-supplied phone (or email) with no invocation of the plugin's own customerIdentityConfirmed() predicate. When a site owner has placed the supported {client_name}, {client_email}, {client_phone}, or {client_note} placeholders into the Details step's Appearance information text, the matched customer's stored name, email, phone and internal notes are substituted into the returned HTML. This makes it possible for unauthenticated attackers who know only a registered customer's primary phone (or email) to read that customer's stored personal data.	5.3	More Details
CVE-2026-108748	Quarkus LangChain4j 1.9.0 through 1.14.1 contains a missing release of memory vulnerability in the chat-scopes WebSocket /_chat/routes endpoint that allows unauthenticated remote clients to exhaust server memory. Attackers can send repeated CONNECT frames reusing one chatId, leaving orphaned scopes in activeScopes until the JVM exits and degrading availability.	5.3	More Details
CVE-2026-103517	The Airwallex Online Payments Gateway WordPress plugin before 1.36.0 does not verify that an incoming payment notification genuinely comes from the payment provider when no webhook secret has been configured, allowing unauthenticated attackers to forge one and mark orders as paid without paying.	5.3	More Details
CVE-2026-62128	Missing Authorization vulnerability in Creator LMS Creator LMS creatorlms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Creator LMS: from n/a through 1.2.21.	5.3	More Details
CVE-2026-108862	APIPark through 1.9.7-beta contains an insecure direct object reference vulnerability that allows authenticated users to read other applications' credentials by supplying a foreign authorization UUID. Attackers with authorization-view permission on one application can query /api/v1/app/authorization or its details route to retrieve plaintext API keys regardless of HideCredential.	5.3	More Details
CVE-2026-105190	The Easy Digital Downloads WordPress plugin before 3.7.1 does not consult the site's user registration setting before creating a WordPress account, allowing unauthenticated users to create an account and receive a logged-in session even when registration is disabled. The created account receives the site's default role.	5.3	More Details
CVE-2026-104671	The TutorStarter WordPress theme before 4.0.4 does not respect the site's user registration setting in one of its AJAX registration handlers, allowing unauthenticated visitors to create WordPress user accounts even when user registration is disabled.	5.3	More Details
CVE-2026-108102	Open5GS through 2.8.0 contains a heap out-of-bounds read vulnerability in ogs_pfcparse_volume_measurement() in lib/pfcparse/types.c that allows remote unauthenticated attackers to read past IE buffers. Attackers can send a PFCP Session Report Request to the SMF on UDP port 8805 with a short, all-flags Volume Measurement IE, reading up to 48 bytes and potentially crashing the SMF.	5.3	More Details
CVE-2026-6723	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Incorrect Authorization in all versions up to, and including, 1.6.11.11. This is due to the appointment update REST API endpoint not restricting which fields can be modified by token-authenticated customers. This makes it possible for unauthenticated attackers to modify admin-controlled fields on that appointment, including faking payment confirmation, reassigning the appointment to another user, and changing the service type.	5.3	More Details
CVE-2026-106600	Missing Authorization vulnerability in Liquid Web / StellarWP GiveWP give allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GiveWP: from n/a through 4.18.0.	5.3	More Details
CVE-2026-16177	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 could allow a remote authenticated attacker to obtain sensitive information due to an out-of-bounds read.	5.3	More Details
CVE-2026-107834	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. From 3.0.0 until 3.8.0, the multipart loop in internal/bodyprocessors/multipart.go executes defer temp.Close() for every uploaded file part, so each temporary-file descriptor remains open until the complete request returns. An unauthenticated attacker can submit a multipart body containing many minimal file parts and exhaust the process file-descriptor table within the request-body size limit, causing os.CreateTemp failures, MULTIPART_STRICT_ERROR responses, blocked legitimate uploads, and process-wide inability to open files or sockets. This issue is fixed in version 3.8.0.	5.3	More Details
CVE-	The Booking Package WordPress plugin before 1.7.30 does not perform authorization checks before returning		More

2026-105995	stored reservation data, allowing unauthenticated users to disclose other customers' personal information and booking cancellation tokens.	5.3	Details
CVE-2026-108584	A security flaw has been discovered in FunnyWolf Viper up to 3.1.11. The affected element is an unknown function of the file /root/viper/.git/config. Performing a manipulation results in hard-coded credentials. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	5.3	More Details
CVE-2026-75597	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev101, the <code>`/web/<path:filename>`</code> route in <code>`src/pyload/webui/app/blueprints/app_blueprint.py`</code> renders Jinja2 templates without any authentication requirement. Every equivalent direct route (<code>`/logs`</code> , <code>`/settings`</code> , <code>`/queue`</code> , <code>`/dashboard`</code> , etc.) is protected by <code>`@login_required`</code> , but the underlying templates for all of these pages are accessible unauthenticated via this endpoint. Combined with an exception attribute typo in <code>`src/pyload/webui/app/handlers.py`</code> (<code>`exc.desc`</code> instead of <code>`exc.description`</code>), internal Jinja2 variable names are leaked in HTTP 500 response bodies to unauthenticated callers. An attacker can also enumerate all valid template names by observing 200 vs 500 response differentiation. Version 0.5.0b3.dev101 contains a patch.	5.3	More Details
CVE-2026-108724	Sylius through 2.3.0 contains an authorization bypass vulnerability that allows unauthenticated attackers to read unmoderated and rejected product reviews because the AcceptedExtension filter is not applied to the item operation. Attackers can enumerate sequential ids on GET <code>/api/v2/shop/product-reviews/{id}</code> to retrieve review titles, ratings, comments, timestamps and author first names, bypassing merchant moderation.	5.3	More Details
CVE-2026-105878	Missing Authorization vulnerability in YITH YITH WooCommerce Product Bundles yith-woocommerce-product-bundles allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YITH WooCommerce Product Bundles: from n/a through 2.29.0.	5.3	More Details
CVE-2026-107120	The Contest Gallery WordPress plugin before 33.0.1 does not limit the number of attempts against its front-end registration email-verification step, which relies on a short numeric PIN, allowing unauthenticated attackers to brute-force the PIN and create and activate a WordPress account bound to an email address they do not own, gaining an authenticated session.	5.3	More Details
CVE-2026-105893	Authorization Bypass Through User-Controlled Key vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Manipulating User-Controlled Variables.This issue affects Event Tickets: from n/a through 5.30.0.1.	5.3	More Details
CVE-2026-108850	Company Research Agent through 2.2.0 contains a server-side request forgery vulnerability that allows unauthenticated attackers to trigger outbound requests by injecting unescaped ReportLab paragraph markup into the /generate-pdf endpoint. Attackers can embed inline img elements in report_content to make the server fetch internal or external hosts, leaking image responses in returned PDFs and probing reachability.	5.3	More Details
CVE-2026-42698	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Themeum Tutor LMS tutor allows Leveraging Race Conditions.This issue affects Tutor LMS: from n/a through 4.1.1.	5.3	More Details
CVE-2026-105990	The Accept PayPal Payments using Contact Form 7 WordPress plugin before 4.0.7 does not perform any authorization checks before exporting stored form submissions, allowing unauthenticated attackers to download the personal data (name, email, telephone, postal address, message) and payment metadata of everyone who submitted a payment form.	5.3	More Details
CVE-2026-105989	The Accept PayPal Payments using Contact Form 7 WordPress plugin before 4.0.7 does not perform any authorization or request-validation checks on one of its AJAX actions, allowing unauthenticated attackers to forge the stored transaction status of records and to write the Accept PayPal Payments using Contact Form 7 WordPress plugin before 4.0.7's status metadata onto arbitrary posts.	5.3	More Details
CVE-2026-78013	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Initialization of a Resource with an Insecure Default vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service, Information disclosure, and Protection mechanism bypass.	5.2	More Details
CVE-2026-107888	OpenPrinting CUPS before 2.4.20 contains a NULL pointer dereference in cupsdCheckJobs() when a job marked job-held-on-create refers to a temporary printer that has been automatically deleted. Temporary-printer cleanup can remove the destination without canceling its held jobs, and the scheduler dereferences the NULL result of cupsdFindDest() while checking holding_new_jobs. This terminates cupsd and interrupts all queues managed by that process. In some plausible scenarios, an unprivileged submission can trigger this.	5.1	More Details
CVE-2026-106571	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 6.9.13-56 and 7.1.2-31, a crafted local call to the GetVirtualPixels API can trigger an integer calculation error and write beyond a heap buffer, crashing the server process. This issue is fixed in versions 6.9.13-56 and 7.1.2-31.	5.1	More Details
CVE-2026-	IBM Guardium Data Protection 12.0, 12.1, 12.2 is affected by an improper validation of user-supplied pointers in the WfpMonitor kernel driver. Certain METHOD_NEITHER IOCTL handlers dereference user-controlled	5.1	More

84290	pointers without adequate probing and exception handling, potentially allowing a privileged local attacker to cause a system crash or perform limited kernel-memory reads.		Details
CVE-2026-107565	A flaw was found in luksmeta. A local attacker with administrative privileges can cause data corruption when saving metadata to a Linux Unified Key Setup (LUKS) device. Due to incorrect boundary calculations and flawed overlap detection, new metadata entries can be written beyond available free space or over existing records. This issue can corrupt stored encrypted payload data or existing metadata, potentially rendering the affected data inaccessible.	5.1	More Details
CVE-2026-106435	The MongoDB Python Driver's binary accelerator can read outside a buffer when an application decodes malformed BSON containing a truncated regular-expression element without a trailing NUL byte. An actor who can supply BSON to the documented decode or decode_all API can cause the application process to terminate when the C extension is loaded. The driver's normal database wire-protocol path does not reach this code.	5.1	More Details
CVE-2026-103870	A flaw was found in pulp-rpm when it publishes a distribution tree. Addon and variant ids from .treeinfo are used as directory names. A user who can sync or upload that tree can make the publish task create a new directory outside the task work area and write that tree's repository metadata and packages there, as the Pulp worker user. An existing file or directory is not replaced. The flaw does not disclose data and does not stop the service.	5.0	More Details
CVE-2026-106561	Backstage is an open framework for building developer portals. Prior to 0.21.9, the @backstage/plugin-kubernetes-backend package is affected by sensitive information disclosure in kubernetes resource queries. An authenticated user holding the standard Kubernetes resource read permission could retrieve sensitive values that the Kubernetes plugin is designed to mask, potentially exposing credentials and other confidential material held in the connected clusters. Exposure is limited to resources that the Backstage service account is permitted to read and that match the targeted catalog entity's namespace and label selector. Deployments whose cluster credentials do not grant read access to these resources are unaffected. This issue is fixed in version 0.21.9.	5.0	More Details
CVE-2026-108719	LLMGateway through 1.20.0 contains a blind server-side request forgery vulnerability that allows API key holders to reach internal hosts via the video-generation callback_url extension. Attackers can supply loopback, private, or cloud-metadata URLs that deliverWebhook POSTs to without the assertSafeWebhookTarget check, reaching internal services from the worker's network.	5.0	More Details
CVE-2026-14521	IBM DataPower Gateway 10.5.0.0 through 10.5.0.22, 10.6.1 through 10.6.6, 10.6.0.0 through 10.6.0.10, and 11.0.0.0 through 11.0.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	4.9	More Details
CVE-2026-76452	A vulnerability in the web-based management interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an authenticated, remote attacker to conduct SQL injection attacks against an affected application. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to read additional contents of the internal database of an affected application that should not normally be accessible to administrative users, thus impacting system confidentiality. To exploit this vulnerability, the attacker must have valid administrative user credentials on the affected application.	4.9	More Details
CVE-2026-107708	MIT krb5 through 1.22.2 contains a NULL pointer dereference vulnerability in the KDC's get_pac Princ_with_realm() that returns success while leaving the client principal NULL on malformed names. A malicious or compromised cross-realm trusted KDC can send an S4U2Proxy request with a PAC carrying a malformed client name to crash krb5kdc and deny authentication.	4.9	More Details
CVE-2025-71428	Jivejdon through 5.0 contains a sql injection vulnerability in AccountDaoSql.getAccountByNameLike() that allows authenticated administrators to inject SQL via the username parameter. Attackers with the Admin role can submit crafted input to /admin/user/userListAction to read database contents, including other accounts' password hashes.	4.9	More Details
CVE-2026-108124	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in wp-post-author. This issue affects wp-post-author before 4.1.0.	4.9	More Details
CVE-2026-104023	The Smart Popup by Supsysytc plugin for WordPress is vulnerable to generic SQL Injection via the 'sidx' parameter in all versions up to, and including, 1.13.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-	The Listdom: AI-powered Business Directory with Classifieds Ads Listings plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the LSD_Menus_IX_CSV::import function in all versions up to, and including, 6.1.2 This makes it possible for authenticated attackers, with administrator-	4.9	More Details

104722	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).		
CVE-2026-108115	Kortix Suna 0.10.7 before 0.13.52 contains a server-side request forgery vulnerability that allows project managers to bypass the isPrivately guard by supplying IPv6 6to4 or Teredo addresses that embed private IPv4 destinations. Attackers holding project.connector.write can set connector base_url, OpenAPI, Postman, or MCP URLs to reach internal services and cloud metadata endpoints and read responses.	4.9	More Details
CVE-2026-11936	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 local management interface in certain configurations 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.	4.9	More Details
CVE-2026-104763	The Post Export Import with Media plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.17.1 via the 'file_path' parameter parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. This requires the attacker to upload a crafted ZIP archive containing a media_metadata.json file with path traversal sequences in the file_path field while specifying an allowed file extension for the destination filename to bypass the extension guard introduced in version 1.13.2.	4.9	More Details
CVE-2026-96396	The Affinity by Canva application for macOS before 3.3.1 (October 2026 release) did not safely calculate the size of an image buffer when generating QuickLook thumbnails and previews of Affinity document files, leading to an integer overflow and a heap-based buffer overflow. A threat actor could craft an Affinity document that, when displayed or previewed by a user in Finder, could corrupt heap memory and cause the thumbnail or preview extension to crash.	4.9	More Details
CVE-2026-33272	A malicious user with physical access to the device can boot the switch from factory settings without authentication, use the default administrative credentials to obtain administrative access, and save changes to the configuration file so that they persist next time the switch boots normally.	4.9	More Details
CVE-2026-107604	A flaw was found in the installation provider and client registration endpoints of the Keycloak identity management service. A realm administrator with only the read-only view-clients role can access the active primary secret of any confidential client, which should normally be restricted. This exposed secret can be used to impersonate the client and gain unauthorized access to its associated service account permissions.	4.9	More Details
CVE-2026-76437	A vulnerability in the web-based user interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper validation of user-supplied content within configurations that are submitted to the web-based management interface. An attacker could exploit this vulnerability by updating configurations within the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. To exploit this vulnerability, the attacker must have valid administrative credentials. Because only an attacker who already holds system administrator privileges can exploit the vulnerability, the only additional privileges gained include the ability to turn off the system, which an administrative user could not normally do.	4.9	More Details
CVE-2026-108104	Xerial snappy-java from 1.1.7.4 before 1.1.10.10 contains a double release vulnerability in SnappyFramedInputStream that returns pooled buffers twice when replacement allocation fails. Attackers can supply framed data with a large declared chunk length to trigger OutOfMemoryError, causing shared backing arrays that expose or overwrite other streams' decompressed data.	4.8	More Details
CVE-2026-106436	The BSON encoder in the MongoDB PHP Driver does not check some return values after a document exceeds libbson's size limit. This can leave the encoder in an invalid state. An unauthenticated actor who can cause an affected application to encode an unusually large data structure can terminate the PHP worker or cause the resulting document to omit fields. No MongoDB server connection or database authentication is required.	4.8	More Details
CVE-2026-105193	The Booking Calendar WordPress plugin before 11.8 does not generate its per-booking access hashes with sufficient entropy, deriving each from a low-entropy time-seeded value, which can allow unauthenticated attackers who are able to determine a booking's creation time to predict the hash and then read that booking's personal data or modify the booking in place.	4.8	More Details
CVE-2026-108597	Cohere Python SDK 5.11.0 through 7.2.0 contains a path traversal (tar slip) vulnerability in _s3_models_dir_to_tarfile that allows arbitrary file write via unvalidated tarfile.extractall calls. Attackers who can write model archives to the victim's S3 prefix can include absolute paths or ../ members to overwrite files on the SDK host.	4.8	More Details
CVE-2026-107660	FFmpeg before 8.1.3 and 9.x before 9.0.2 contains an improper certificate validation vulnerability in tls_open() of libavformat/tls_mbedtls.c, which skips hostname checks for IP-address hosts. Network attackers can intercept https, rtmps, or tls connections to IP-literal URLs with any trusted CA-issued certificate to read and tamper with streams.	4.8	More Details
	wger is a free, open-source workout and fitness manager. Versions prior to 2.6 have a vulnerability in the authentication/session lifecycle of `wger` where bearer-style API credentials remain valid after a user logs		

CVE-2026-46437	out and after a user changes their password. An attacker who steals a victim's DRF authtoken (`Authorization: Token ...`) or JWT refresh token can continue to access protected `/api/v2/*` endpoints until the token is manually rotated/deleted (DRF token) or naturally expires (JWT refresh). Version 2.6 contains a patch.	4.8	More Details
CVE-2026-84220	The Kirki WordPress plugin before 6.3.2 does not prevent shortcodes held in comments from being executed when it renders them, and displays comments regardless of their moderation status, allowing unauthenticated visitors to run shortcodes registered on the site and to read private custom fields of the page being viewed.	4.8	More Details
CVE-2026-106602	Authentication Bypass Using an Alternate Path or Channel vulnerability in Automattic Jetpack jetpack allows Password Recovery Exploitation.This issue affects Jetpack: from n/a through 16.2.	4.8	More Details
CVE-2026-19735	The RFC 6528 initial-sequence-number implementation in subsys/net/ip/tcp.c derived every TCP ISN from SHA-256(unique_key four-tuple) plus a uptime-derived offset, where unique_key is a 128-bit secret filled once by sys_csrand_get(). The return value of that call was discarded and the once guard was latched to true even when the call failed. Because sys_csrand_get() leaves the destination buffer untouched on failure (it deliberately propagates the entropy-driver error rather than filling the buffer), a single failed call left unique_key as its all-zero BSS content for the remainder of the boot, with no retry, no log message and no fallback. A failure of the cryptographic random source is required to reach the weak state — for example - ENODEV/-EIO from the entropy driver in subsys/random/random_entropy_device.c (the in-tree comment notes that the hardware RNG "might still be gathering entropy during early boot situations"), or psa_generate_random() failing in subsys/random/random_psa.c when PSA crypto is not initialised or is backed by a Bluetooth-HCI entropy device that is not yet up. The first TCP connection is what triggers key generation, so a remote peer that reaches a listening port immediately after boot, or that can provoke a reboot, has indirect influence over whether generation coincides with that window. tcp_init_isn() is called for every passive open in tcp_conn_new() and every active open in net_tcp_connect(), so the poisoned key governs all TCP connections for that boot. With an all-zero key the ISN becomes a public function of the connection four-tuple plus a device-wide time offset. An off-path attacker can compute the hash term offline for any four-tuple and recover the shared time offset from a single observed ISN, after which the ISN the device will pick for other four-tuples is predictable. That defeats exactly the protection RFC 6528 provides: blind TCP connection spoofing against peers that trust the source address, and blind data injection into or reset of connections whose four-tuple can be guessed. Devices whose entropy source never errors were never in the weak state. The fix moves key generation into a single guarded helper that latches only on success, logs the error otherwise, and makes tcp_init_isn() fall back to sys_rand32_get() — the behaviour already used when CONFIG_NET_TCP_ISN_RFC6528 is disabled — instead of hashing with a known-constant key.	4.8	More Details
CVE-2026-48212	An OTRS administrator can enter arbitrary JavaScript into the content of an OTRS Custom Page, which is stored by the application and subsequently executed in the browser of users accessing that page. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X	4.8	More Details
CVE-2026-107272	Gophish through 0.12.1 contains stored and reflected cross-site scripting vulnerabilities that allow attackers to inject script by returning malicious SMTP server error messages. Attackers controlling or intercepting a sending profile's SMTP server can execute script when administrators view campaign results or send test emails, stealing API keys.	4.7	More Details
CVE-2026-108521	A vulnerability has been found in Studio-Saelix Sencho up to 0.97.1. Affected by this issue is the function isValidRemoteUrl of the file backend/src/utills/validation.ts of the component Add Remote Node API Endpoint. Such manipulation leads to server-side request forgery. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor confirms: "The node API URL could be configured by an authenticated user with node-management permission and used to initiate server-side requests. [T]he report demonstrates server-side request capability but not arbitrary internal response exfiltration."	4.7	More Details
CVE-2026-108600	open-multi-agent (@open-multi-agent/core) 1.5.0 through 1.21.2 contains a link following vulnerability in the file_write tool sandbox that allows attackers to create files outside the workspace root by using dangling symlinks. Attackers can plant a dangling symlink in the workspace and steer the agent via prompt injection to write attacker-influenced content anywhere the agent process can write.	4.7	More Details
CVE-2026-101324	The Fluent Forms - Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'any attacker-chosen name matching the {get.NAME} placeholder (PoC uses 'proof')' parameter in all versions up to, and including, 6.2.14 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. Exploitation requires a site administrator to have configured a Custom HTML field on a published form containing a {get.*} SmartCode inside a URL-accepting attribute such as iframe src or a href — a documented Fluent Forms feature.	4.7	More Details
CVE-	A security flaw has been discovered in Zen Cart up to 2.2.2. Affected by this issue is some unknown functionality of the file admin/modules.php of the component Module Configuration. The manipulation of the		More

2026-108829	argument configuration results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The patch is identified as 08f572654edee1db8f9db091c9949825c6c69339. It is advisable to implement a patch to correct this issue.	4.7	Details
CVE-2026-108852	Deep Chat through 2.5.1 contains a cross-site scripting vulnerability that allows attackers to inject javascript: links because RemarkableConfig.createNew disables Remarkable link validation. Attackers can place crafted Markdown links in AI responses, addMessage content, or loaded history to execute script in the embedding page when victims click them.	4.7	More Details
CVE-2026-108599	phi 0.1.1 through 0.28.4 contains an improper link resolution vulnerability that allows malicious repositories to bypass workspace_only_writes by exploiting lexical-only path checks in the permission gate. Attackers can commit symlinks pointing outside the workspace and use prompt injection to make the write tool write attacker-influenced content to external files without approval.	4.7	More Details
CVE-2026-107678	FFmpeg through 9.0.2 contains a stack exhaustion vulnerability in av_encryption_init_info_free() in libavutil/encryption_info.c, which recursively frees AVEncryptionInitInfo linked lists built by the MOV demuxer's mov_read_pssh(). Attackers can supply a crafted MP4 file with tens of thousands of small pssh boxes to exhaust the stack and crash the process, while also causing quadratic CPU consumption.	4.7	More Details
CVE-2026-103912	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Reflected DOM-Based Cross-Site Scripting via the '<attacker-chosen query var name matching the preset's query_var setting>' parameter in all versions up to, and including, 3.6.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is only exploitable on pages embedding a form that has a text field configured with a query_var Dynamic Preset and a data-jfb-macro or JFB_FIELD:: macro reference targeting that field, both of which are standard, documented plugin features.	4.7	More Details
CVE-2026-107677	FFmpeg through 9.0.2 contains a denial of service vulnerability in the DASH demuxer that allows attackers to trigger an infinite loop by supplying an empty SegmentTemplate media URL. Attackers can craft an .mpd manifest declaring SegmentTemplate media="" so get_current_fragment() calls av_strireplace() with an empty search string, consuming CPU indefinitely.	4.7	More Details
CVE-2026-101921	The WPForms – AI Form Builder for WordPress – Contact Forms, Payment Forms, Survey Form, Quiz & More plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'attacker-chosen key referenced by the smart tag (e.g. "x")' parameter in all versions up to, and including, 2.0.2.1 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. Exploitation requires that a site administrator has previously saved a form whose description embeds a {query_var} Smart Tag inside an iframe srcdoc attribute and has enabled Show Description on a public-facing page.	4.7	More Details
CVE-2026-105976	The Portfolio Filter Gallery WordPress plugin before 2.2.1 does not perform proper authorization checks in a set of AJAX actions, allowing users with at least the Contributor role to read, modify and delete other users' galleries as well as site-wide gallery filters.	4.7	More Details
CVE-2026-88785	The Simple Membership WordPress plugin before 4.8.3 does not avoid transmitting a newly registered member's plaintext password in a URL query string when an optional auto-login-after-registration feature is enabled, exposing the credential in browser history and in web server, proxy, and CDN access logs to anyone able to read them.	4.7	More Details
CVE-2026-108790	A security flaw has been discovered in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c355668fc8dab. This impacts the function TemplateController.save of the file /system/cms/template/save of the component Backend Template Editor. The manipulation results in path traversal. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-108952	RT-Thread through 5.3.0 contains a memory corruption vulnerability in the legacy USB CDC virtual COM port driver that aliases rx_ringbuffer as a Serial V2 rt_serial_rx_fifo in _function_enable(). A connected USB host configuring the CDC device triggers writes past the ring buffer into struct vcom members and an invalid rt_free() on close, causing denial of service.	4.6	More Details
CVE-2026-107856	CiviForm simplifies applications for government benefits programs by reusing applicant data across multiple benefit applications. Prior to 3.33.0, GET /admin/tiDash/editClientForm/:accountId verifies that the requester is a Trusted Intermediary but showEditClientForm performs a raw lookupAccount(accountId) without confirming that the citizen account belongs to the requester's trustedIntermediaryGroup. An authenticated Trusted Intermediary can enumerate accountId values and read the applicant display name, including the citizen's name and email address, for accounts outside the intermediary's group. This issue is fixed in version 3.33.0.	4.5	More Details
CVE-2026-	The Affinity by Canva application before 3.3.1 (October 2026 release) did not perform adequate bounds checking when parsing raster image data in Affinity document files, leading to an out-of-bounds read and the dereference of an untrusted pointer. A threat actor could craft an Affinity document that, when opened by a	4.5	More Details

103220	user in Affinity, could result in memory corruption or an application crash.		
CVE-2026-107857	Mindwtr is a free offline-first task management application for desktop and mobile. Prior to 1.1.5, the mobile application writes the Cloud sync bearer token and WebDAV password to unencrypted AsyncStorage under @mindwtr_cloud_token and @mindwtr_webdav_password. A party with access to the application database or an exposed device backup can recover these credentials and use them to access the user's synchronized tasks and attachments. This issue is fixed in version 1.1.5.	4.4	More Details
CVE-2026-107817	MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the mysql_json plugin assumed that imported MySQL tables contained valid MySQL binary JSON data. A specially prepared MySQL table containing invalid JSON data could cause out-of-bounds reads, information disclosure, or a server crash. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	4.4	More Details
CVE-2026-108835	A flaw has been found in Yungengxin Yun Jia Security Guard up to 2.7.1.9. Impacted is the function sub_14000885C in the library kgameprotect.sys. Executing a manipulation of the argument Pid can lead to improper privilege management. The attack requires local access. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2026-107397	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to 3.3.13, users who can create content, including speakers who can create minutes, can store crafted HTML in event minutes. When concurrent edits are made to the same minutes, the minute editor conflict UI can execute attacker-controlled script in the viewer's browser in the Indico origin. This issue is fixed in version 3.3.13.	4.4	More Details
CVE-2026-108591	InnoShop 0.9.2 contains a local file disclosure vulnerability that allows authenticated administrators with files_create permission to read server files by abusing the AI Core MCP file_upload tool's source argument. Attackers can supply file:// or php:// stream wrappers passed to file_get_contents(), storing contents on the public media disk to expose the .env file with APP_KEY and database credentials.	4.4	More Details
CVE-2026-108889	A flaw has been found in Yungengxin Cloud Billing 2024.11.28.11. Affected by this vulnerability is the function sub_14000443C in the library LWBilling64.sys of the component IOCTL Process Termination. Executing a manipulation of the argument Pid can lead to exposed ioctl with insufficient access control. The attack needs to be launched locally. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2026-108751	MoAI-ADK through 3.1.2 contains an improper link resolution vulnerability in the moai init template deployer that allows malicious repositories to overwrite files outside the project via a symlinked .moai-tmp staging path. Attackers can commit a symlink such as .claude/settings.json.moai-tmp so atomicWriteFile truncates and overwrites victim-writable files with MoAI template content.	4.4	More Details
CVE-2026-103897	The Responsive Lightbox & Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 2.7.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the plugin's 'Comments' lightbox setting to be enabled (disabled by default), a moderator to approve the injected comment, and a site visitor to click the affected image to open the lightbox.	4.4	More Details
CVE-2026-44034	A heap-based out-of-bounds read in DcmRLECodecDecoder::decodeFrame() in dcldata/libsrc/dcrleccd.cc of OFFIS DCMCTK 3.7.0 allows an attacker to read up to 63 bytes of adjacent heap memory, or cause a crash, via a crafted RLE Lossless DICOM file whose pixel data fragment is shorter than the 64-byte RLE header. The function copies 64 bytes without checking the fragment length, a check that the sibling function decode() already performs. Applications that decode RLE images frame by frame (for example, through DcmPixelData::getUncompressedFrame()) are affected. The dcmdrle command-line tool uses decode() and is not affected. The issue is fixed in commit 45469f3c30037e9c7159290e4bb74cd7b3b9ef1d.	4.4	More Details
CVE-2026-20032	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, local attacker with low privileges to escape the Python sandbox and gain unauthorized access to the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user.	4.4	More Details
CVE-2026-44038	A global out-of-bounds read in the Huffman decoder of the bundled IJG JPEG libraries (dcmjpeg/libijg8, libijg12 and libijg16) of OFFIS DCMCTK 3.7.0 allows an attacker to read memory beyond the extend_test[] and extend_offset[] tables, causing incorrectly decoded pixel data or a crash, via a DICOM file with a crafted JPEG stream whose Huffman table defines a difference category above 15. Huffman symbol values are not range-checked unless DCMCTK is built with DCMCTK_ENABLE_STRICT_HUFFMAN_TABLE_CHECK, which is disabled by default. dcmdjpeg and any application that decompresses JPEG DICOM images with DCMCTK are affected. The issue is fixed in commit d6ae1bc8d5b9ae9c7300013c8c85cc2ea0fd8cf5.	4.4	More Details

CVE-2026-105139	Obot 0.26.0 before 0.26.2 contains an authorization bypass vulnerability that allows authenticated users matching any vMCP profile to reach prompts and resources of ungranted components. Because profiles were enforced only on tools, attackers can access prompts, resources, and resource templates through the vMCP owner's shared component connection.	4.3	More Details
CVE-2026-108646	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysCategoryController importExcel handler that allows any authenticated user to import category dictionary entries. Low-privileged attackers can upload crafted Excel workbooks to bulk insert arbitrary nodes into the system-wide sys_category dictionary, including under existing parent nodes.	4.3	More Details
CVE-2026-108647	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to create validation rules through the SysCheckRuleController importExcel handler. Attackers can upload a crafted Excel workbook to bypass the system:checkRule:add permission and bulk-create system-wide encoding validation rules with arbitrary regular expression patterns.	4.3	More Details
CVE-2026-109173	yshop-crm through 2.1.3 contains a missing authorization vulnerability that allows any authenticated back-office user to approve or reject invoices via POST /admin-api/crm/invoice/check. The CrmInvoiceController check handler lacks @PreAuthorize and approver checks are commented out, letting attackers bypass the invoice approval workflow by supplying any invoice id.	4.3	More Details
CVE-2026-108645	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in SysCategoryController that allows any authenticated user to edit category dictionary nodes via /sys/category/edit. Low-privileged attackers can send POST or PUT requests supplying a node id to rename, recode, or move system-wide sys_category nodes, altering classification values used across forms.	4.3	More Details
CVE-2026-108713	SuiteCRM through 7.15.2 and 8.x through 8.10.2 contains a missing authorization vulnerability that allows authenticated users to create and modify EmailMarketing records via the setCampaignMarketingAndTemplate entry point. Low-privileged users denied Campaigns access can post marketingId, campaignId, and templateId to reattach marketing messages or swap the template EmailMan sends in campaign emails.	4.3	More Details
CVE-2026-108658	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysTenantController queryTenantAuthInfo handler that allows any authenticated user to read other tenants' records. Low-privileged attackers can iterate small integer tenant ids to retrieve full sys_tenant records, including house numbers used as tenant join codes and company profile fields.	4.3	More Details
CVE-2026-109175	MoguBlog through 6.2 contains an insecure direct object reference vulnerability that allows authenticated administrators to list other administrators' network-disk files via POST /networkDisk/getFileList. Attackers can query the endpoint, which filters only by status, file type, or filePath and never by admin_uid, to obtain other administrators' file names and download URLs.	4.3	More Details
CVE-2026-108659	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysTenantController listPackByTenantUserId handler that allows any authenticated user to query tenant product packs. Low-privileged attackers can supply arbitrary tenantId and userId parameters to enumerate any tenant's product pack configuration and reveal which users are tenant administrators.	4.3	More Details
CVE-2026-108834	A vulnerability was detected in Cairo-dock Glx-Dock up to 3.4.0. This issue affects some unknown processing of the file ww_page.php of the component Query Parameter Handler. Performing a manipulation of the argument p results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-108649	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the queryUserRolesById handler of SystemApiController that lets authenticated users read any user's role codes. Low-privileged attackers can send a userId to GET /sys/api/queryUserRolesById to enumerate role assignments and identify administrator accounts.	4.3	More Details
CVE-2026-109172	yshop-crm through 2.1.3 contains a missing authorization vulnerability that allows any authenticated back-office user to approve or reject receivables records by calling POST /admin-api/crm/contract-receivables/check. The handler lacks a @PreAuthorize check and the approver checks in CrmContractReceivablesServiceImpl.check are commented out, so attackers can approve records by id, inflating contract return_money and forging approval logs.	4.3	More Details
CVE-2026-109171	yshop-crm through 2.1.3 contains a missing authorization vulnerability that allows any authenticated back-office user to approve or reject contracts by calling POST /admin-api/crm/contract/check. Because CrmContractController lacks @PreAuthorize and approver checks are commented out, attackers can approve contracts to alter customer deal and purchase data or reject them to return products to stock.	4.3	More Details
CVE-2026-109167	TDuck survey form through 6.0 contains an insecure direct object reference vulnerability in the saveFormTheme handler that allows authenticated users to overwrite other users' form themes. Attackers whose form has no theme can submit another form's sequential theme id with their own formKey, replacing its colours and image URLs and removing the victim's theme.	4.3	More Details

CVE-2026-108650	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the getUserPermissionSet handler of SystemApiController that allows any authenticated user to read other users' permission codes. Low-privileged attackers can supply an arbitrary userId to GET /sys/api/getUserPermissionSet to retrieve the full permission set of any account, including administrators.	4.3	More Details
CVE-2026-109165	TDuck survey form through 6.0 contains a broken access control vulnerability that allows authenticated users to add fields to other users' forms via POST /user/form/item/batch/create. Attackers can submit an array whose first element references their own form and later elements reference a victim's formKey, injecting attacker-chosen fields onto the victim's public fill page.	4.3	More Details
CVE-2026-97183	The WP-Invoice WordPress plugin through 4.3.1 does not perform capability checks in several of its AJAX handlers, allowing any authenticated user, such as a Subscriber, to retrieve the email addresses, display names and profile details of all registered users.	4.3	More Details
CVE-2026-108651	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the getRolesByUserId handler of SystemApiController that allows authenticated users to retrieve any user's role codes. Low-privileged attackers can supply arbitrary userId values to GET /sys/api/getRolesByUserId to enumerate role assignments and identify administrator accounts.	4.3	More Details
CVE-2026-108652	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SystemApiController updateAvatar handler that allows any authenticated user to change other users' avatars. Low-privileged attackers can send PUT requests with a target user id and an arbitrary value, such as an attacker-controlled image URL, to replace administrators' avatars.	4.3	More Details
CVE-2026-108712	SuiteCRM through 7.15.2 and 8.10.2 contains a missing authorization vulnerability in the DetailUserRole entry point that allows authenticated non-admin users to view other users' ACL data. Attackers can supply another non-admin user's id in the record parameter to read that user's assigned roles and per-module ACL action matrix.	4.3	More Details
CVE-2026-108653	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the queryPageList handler of OpenApiController that allows any authenticated user to list OpenAPI registry definitions. Low-privileged attackers can query GET /openapi/list to read virtual paths, internal origin URLs, IP whitelists, and header and parameter templates intended for administrators.	4.3	More Details
CVE-2026-108654	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the OssFileController queryById handler that allows low-privileged authenticated users to read object storage file records. Attackers who know a record id can request GET /sys/oss/file/queryById to obtain original file names and direct storage URLs of files uploaded by other users.	4.3	More Details
CVE-2026-108655	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the QuartzJobController queryById handler that allows low-privileged authenticated users to read scheduled job records. Attackers can request GET /sys/quartzjob/queryById with a job id to retrieve job class names, cron expressions, job parameters and status reserved for administrators.	4.3	More Details
CVE-2026-108656	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysTenantController GET /sys/tenant/getTenantPackApplyUsers endpoint that allows any authenticated user to read tenant administrator applications. Low-privileged attackers can iterate the tenantId parameter to retrieve pending applicants' usernames, real names, phone numbers and departments for any tenant.	4.3	More Details
CVE-2026-108874	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to assign or remove department heads by calling PUT /sys/user/changeDepartChargePerson. Low-privileged attackers can supply arbitrary userId, department id, and status values to make any user a department head, widening department-scoped views, or demote existing heads.	4.3	More Details
CVE-2026-108640	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysDepartRoleController queryById handler that lacks Shiro permission annotations. Low-privileged authenticated attackers can request GET /sys/sysDepartRole/queryById with any id to read department role names, codes, descriptions and audit fields.	4.3	More Details
CVE-2026-108642	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in SysAnnouncementSendController that allows authenticated users to modify other users' message delivery records. Attackers can obtain delivery ids from GET /sys/sysAnnouncementSend/list and submit edit requests that overwrite read flags, recipient ids, or linked announcements to hide messages from recipients.	4.3	More Details
CVE-2026-108568	A vulnerability was determined in InstantSoft icms2 up to 2.18.2. The affected element is the function validatePaypalOrder of the file system/controllers/billing/actions/paypal.php of the component Billing Module. Executing a manipulation of the argument bid/sig can lead to insufficient verification of data authenticity. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysDepartPermissionController queryById handler that allows any authenticated user to read department permission records. Low-privileged	4.3	More

108632	attackers can request GET /sys/sysDepartPermission/queryById with arbitrary ids to retrieve depart_id, permission_id and data_rule_ids for any department.		Details
CVE-2026-109184	jshERP through 3.6 contains an improper authorization vulnerability that allows low-privilege authenticated users to read any settlement account ledger by supplying an arbitrary accountId. Attackers restricted to personal or department data scope can query GET /account/findAccountInOutList to view other users' bill numbers, counterparties, amounts and remarks within the tenant.	4.3	More Details
CVE-2026-108768	A vulnerability was identified in zhayujie CowAgent up to 2.2.0. Affected by this issue is the function json.loads of the component Streaming Tool-Call Argument Handler. The manipulation leads to allocation of resources. It is possible to initiate 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.	4.3	More Details
CVE-2026-108572	A security vulnerability has been detected in Casdoor up to 3.164.0/4.10.0. Affected is the function CasP3ProxyValidate of the file controllers/cas.go of the component Proxy Validation. Such manipulation of the argument pgtUrl leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. Upgrading to version 4.11.0 is able to address this issue. The name of the patch is 03c6c9aaa2eda5b085ce128ce0d60b34094efbd9/ada08ecd10cbf158f593dee23a8bab63efecf995. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-108626	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysMessageController queryById handler that allows low-privileged authenticated users to read any message push record. Attackers can supply arbitrary record ids to GET /sys/message/sysMessage/queryById to disclose message content and receiver addresses of other users.	4.3	More Details
CVE-2026-108630	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in SysDepartPermissionController that allows any authenticated user to modify department permission records by calling the edit endpoint. Low-privileged attackers can obtain row ids from the unguarded list endpoint and overwrite depart_id, permission_id and data_rule_ids to alter which menus and data rules departments may delegate.	4.3	More Details
CVE-2026-108574	A flaw has been found in BerriAI LiteLLM up to 1.95.0. Affected by this issue is the function ui_view_session_spend_logs of the file litellm/proxy/spend_tracking/spend_management_endpoints.py of the component Spend Tracking. Executing a manipulation of the argument session_id can lead to authorization bypass. It is possible to launch the attack remotely. The exploit has been published and may be used. Upgrading to version 1.96.0 can resolve this issue. This patch is called 722d9ffa4f6c5ae15702ab9ab2c5f6bf1688308b. The affected component should be upgraded.	4.3	More Details
CVE-2026-109188	jshERP through 3.6 contains a missing authorization vulnerability that allows low-privilege authenticated users to create tenant-wide master data via add and import endpoints lacking role checks. Attackers can send POST requests to endpoints like /account/add, /material/add, or /material/importExcel to create settlement accounts, products with initial stock, departments and dictionary entries.	4.3	More Details
CVE-2026-108629	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the saveDatarule handler of SysDepartPermissionController that allows any authenticated user to modify department data rules. Low-privileged attackers can send departId, permissionId and dataRuleIds to POST /sys/sysDepartPermission/datarule to change, add or clear data rules on any department-menu permission binding.	4.3	More Details
CVE-2026-108886	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysUserController queryChildrenByUsername handler that allows any authenticated user to retrieve other users' account records. Low-privileged attackers can supply arbitrary userId values to obtain names, emails, phone numbers, employee numbers, department assignments, and staff lists of departments those users head.	4.3	More Details
CVE-2026-93679	IBM Langflow OSS 1.0.0 through 1.12.2 could allow a remote authenticated attacker to cause a denial of service due to uncontrolled resource consumption during ZIP file extraction.	4.3	More Details
CVE-2026-108577	A vulnerability was determined in Konstanty Bialkowski libmodplug up to 0.8.9.1. This issue affects the function abc_add_gchord of the file src/load_abc.cpp of the component ABC Music Format Parser. This manipulation causes resource consumption. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-108627	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the loadDatarule handler of SysRoleController that lets any authenticated user query role data rules. Low-privileged attackers can request GET /sys/role/datarule/{permissionId}/{roleId} to read rule names, columns, conditions, values and bound rule ids for any role.	4.3	More Details
CVE-2026-108887	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysCommentController exportXls handler that allows any authenticated user to export all comments. Low-privileged attackers can request /sys/comment/exportXls to download every sys_comment row, including comment text and user ids on records they cannot access.	4.3	More Details

CVE-2026-108888	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysDepartRoleController exportXls handler that allows any authenticated user to export department roles. Low-privileged attackers holding only the default minimal role can call /sys/sysDepartRole/exportXls to download all sys_depart_role records, including role names, codes, descriptions and creating users.	4.3	More Details
CVE-2026-108633	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to create department permission bindings via POST /sys/sysDepartPermission/add. Attackers can submit arbitrary departId, permissionId and dataRuleIds fields to attach menu, button and data rule grants to any department for delegation to its roles.	4.3	More Details
CVE-2026-109183	jshERP through 3.6 contains an authorization bypass vulnerability that allows authenticated users to create pre-approved bills by setting status in POST /depotHead/addDepotHeadAndDetail requests. Attackers can supply a status of 1 to skip audit permission checks and multi-level approval workflows, creating audited bills that affect stock and report queries.	4.3	More Details
CVE-2026-108641	JeecgBoot through 3.9.5 contains an insecure direct object reference vulnerability that allows authenticated users to read other users' in-application messages via the getOne handler of SysAnnouncementSendController. Attackers can obtain delivery record ids from the unguarded /sys/sysAnnouncementSend/list endpoint and supply them as the sendId parameter to retrieve message titles, bodies, senders and recipients.	4.3	More Details
CVE-2026-108635	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the GET /sys/sysDepart/getDepartmentHead endpoint of SysDepartController that allows any authenticated user to list department staff. Low-privileged attackers can enumerate departId values to retrieve staff names, avatars, posts, and mobile and telephone numbers, including contacts marked hidden.	4.3	More Details
CVE-2026-108715	LibreNMS through 26.9.1.1 contains an authorization bypass vulnerability in includes/html/graphs/smokeping/auth.inc.php that checks the src probe device instead of the rendered target device. Restricted users permitted on a probe device can request smokeping_in or smokeping_out graphs with arbitrary device ids to view latency data and enumerate device names.	4.3	More Details
CVE-2026-109177	MoguBlog through 6.2 contains a broken access control vulnerability that allows authenticated administrators to move or rename other administrators' network-disk files by supplying their file paths. Attackers can send crafted requests to POST /networkDisk/moveFile, batchMoveFile, or edit, which update rows without admin_uid checks, relocating or renaming other users' files and folders.	4.3	More Details
CVE-2026-109179	jshERP through 3.6 contains a missing authorization vulnerability in LogController that allows any authenticated user to read the tenant's operation audit log. Low-privilege users can send GET requests to /log/list or /log/info to view other users' login names, client IP addresses, and actions.	4.3	More Details
CVE-2026-108769	A security flaw has been discovered in zhayujie CowAgent up to 2.2.0. This affects an unknown part of the file Markdown.tsx of the component Markdown Rendering. The manipulation results in denial of service. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-109180	jshERP through 3.6 contains an authorization bypass vulnerability that allows authenticated users to read data from unassigned warehouses by supplying depotId or depotIds request parameters. When depot_flag warehouse restriction is enabled, attackers can name arbitrary warehouse ids in endpoints like /depotItem/getMaterialDepotStockByParam to read stock levels, batch numbers, sales figures and priced bill lines within the tenant.	4.3	More Details
CVE-2026-104390	Missing Authorization vulnerability in Arraytics Booktics booktics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booktics: from n/a through 1.0.27.	4.3	More Details
CVE-2026-108711	Plastic Labs Honcho through 3.3.0 contains an incorrect authorization vulnerability that allows peer- or session-scoped API key holders to read workspace data because get_or_create_workspace checks only the workspace claim. Attackers can submit their parent workspace name to the POST /v3/workspaces endpoint to retrieve workspace metadata and configuration, including custom_instructions, reserved for workspace or admin keys.	4.3	More Details
CVE-2026-108567	A vulnerability was found in InstantSoft icms2 up to 2.18.2. Impacted is the function files_delete_file of the file system/fields/image.php of the component Image Handler. Performing a manipulation of the argument size results in path traversal. The attack may be initiated remotely. The exploit has been made public and could be used. The patch is named 03d70937f1ff97031523222808726994b8b79379. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2026-108681	A security flaw has been discovered in zhayujie CowAgent up to 2.1.7. Impacted is an unknown function of the file channel/web/web_channel.py of the component Web Console. The manipulation of the argument session_id results in denial of service. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. Version 2.1.7 (commit dec28324) only partly mitigates via a 512MB body cap. The vendor was contacted early about this disclosure.	4.3	More Details

CVE-2026-109181	jshERP through 3.6 contains an authorization bypass vulnerability that allows authenticated users restricted to personal or department data to list other users' bills by adding a purchaseStatus value. Attackers can include purchaseStatus=0 in the search JSON on GET /depotHead/list, causing DepotHeadService.select to drop the creator filter and expose all tenant purchase, sales and inventory bills.	4.3	More Details
CVE-2026-109182	jshERP through 3.6 contains an incorrect authorization vulnerability in GET /supplier/exportExcel that allows authenticated users to bypass role data scope restrictions enforced by /supplier/list. Attackers restricted to personal or department data can export every supplier, customer and member record, exposing contacts, phone numbers, tax numbers, bank accounts and balances.	4.3	More Details
CVE-2026-108638	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to remove group memberships via the deleteGroupUser handler in SysUserController. Attackers can send DELETE requests with arbitrary groupId and userId values to remove any user from any administrator-maintained user group without ownership or tenant checks.	4.3	More Details
CVE-2026-108637	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to remove user group members by calling DELETE /sys/user/deleteUserGroupBatch. Attackers can supply any groupId and comma-separated userIds to delete sys_ugroup_user rows without permission or tenant checks, tampering with administrator-maintained groups.	4.3	More Details
CVE-2026-108697	CoreShop through 2026.2.2 contains a missing authorization vulnerability that allows low-privileged backend users to list permission-restricted resources because ResourceController listAction skips the isGrantedOr403() check. Authenticated Pimcore users lacking resource permissions can request the generated list routes to enumerate payment providers, carriers, price rules, stores, and tax rules including ids, names, and identifiers.	4.3	More Details
CVE-2026-108636	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysDepartController applImportExcel handler that allows any authenticated user to import departments. Low-privileged attackers can upload a crafted Excel workbook to POST /sys/sysDepart/applImportExcel to create arbitrary sys_depart records in the administrator-maintained department tree.	4.3	More Details
CVE-2026-108660	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to modify tenant settings by calling PUT /sys/tenant/updateApplyStatus. Low-privileged attackers can supply any tenant id to overwrite its applyStatus field, enabling or disabling tenant administrator applications across tenants.	4.3	More Details
CVE-2026-93550	The Veeqo for WooCommerce WordPress plugin through 2.2.8 does not restrict who can trigger its remote bridge-installation process or validate the URL it is given before downloading and extracting it, allowing users with Subscriber-level access and above to make the Veeqo for WooCommerce WordPress plugin through 2.2.8 download and extract an attacker-controlled archive containing arbitrary PHP files into the WordPress root.	4.3	More Details
CVE-2026-108881	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the getTenantPackInfo handler that allows any authenticated user to read other tenants' product pack membership. Low-privileged attackers can supply a tenantId and fixed packCode values such as superAdmin, accountAdmin or appAdmin to disclose administrator usernames, real names, phones and departments.	4.3	More Details
CVE-2026-107273	Gophish 0.11.0 through 0.12.1 contains a server-side request forgery vulnerability that allows authenticated low-privileged users to reach loopback and private hosts via POST /api/import/site. Attackers can submit internal URLs, which the default dialer deny list does not block, to read service responses and enumerate internal hosts and ports through error messages.	4.3	More Details
CVE-2026-108795	A vulnerability was detected in ZKTeco BioTime 9.5.6 Build 20260130.3206. Affected by this issue is some unknown functionality of the file /base/api/systemSettings of the component System Settings API. Performing a manipulation results in improper access controls. The attack can be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-108732	Frappe HR (hrms) before 16.11.0, including all 14.x and 15.x releases through 15.64.3, contains a missing authorization vulnerability in the whitelisted get_account_and_amount method that lets authenticated users read payroll amounts. Attackers without HR roles can call the method over /api/method with enumerable Salary Slip or claim document names to disclose other employees' net pay and loan, advance, and claim balances.	4.3	More Details
CVE-2026-108523	A vulnerability was determined in Studio-Saelix Sencho up to 0.94.1. This vulnerability affects unknown code of the file outboundTarget.ts of the component git-sources Browse API Endpoint. Executing a manipulation of the argument repo_url can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The presence of this vulnerability remains uncertain at this time. This patch is called 79b86ddcd4aefdd6941f098e35990ab397b13c72. It is advisable to implement a patch to correct this issue. The vendor explains: "Git repository access is an intentional, privileged administrative function. Sencho explicitly supports repositories hosted on private LAN, VPC, VPN, CGNAT, and IPv6 ULA networks. The report does not demonstrate a privilege-boundary bypass or access by an unprivileged user. We therefore dispute the CVE characterization of this behavior. As defense in depth, we	4.3	More Details

	have nevertheless hardened repository access. Git HTTPS and SSH connections now validate and pin DNS resolution, reject loopback, link-local, multicast, selected special-use and metadata targets, disable redirects and inherited proxy routing, and retain strict SSH host-key verification."		
CVE-2026-108791	A weakness has been identified in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab. Affected is the function TemplateController.input of the file /system/cms/template/input of the component Template Management. This manipulation of the argument filePath causes path traversal. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-108733	Frappe HR (hrms) before 16.11.0, including all 14.x and 15.x releases through 15.64.3, contains a missing authorization vulnerability in the whitelisted expire_allocation method that allows authenticated users to expire any leave allocation. Attackers without HR roles can name another employee's Leave Allocation in a POST request to zero its allocated leaves and wipe that employee's remaining leave balance.	4.3	More Details
CVE-2026-106562	Backstage is an open framework for building developer portals. Prior to 2.1.6 in @backstage/plugin-search-backend and 1.8.7 in @backstage/plugin-search-backend-module-elasticsearch, search engine permission filtering could return documents denied by policy. An authenticated Backstage user subject to a DENY policy for search document types could receive unauthorized results in deployments with permission.enabled set to true and an Elasticsearch or OpenSearch backend. This issue is fixed in @backstage/plugin-search-backend 2.1.6 and @backstage/plugin-search-backend-module-elasticsearch 1.8.7.	4.3	More Details
CVE-2026-108706	eladmin through commit 55fbf70 contains a missing authorization vulnerability in the downloadS3Storage handler that allows any authenticated user to retrieve stored object URLs without storage permissions. Attackers can enumerate sequential ids against GET /api/s3Storage/download/{id} to collect URLs of all uploaded objects, exposing file contents on publicly readable buckets.	4.3	More Details
CVE-2026-108683	A security vulnerability has been detected in zhayujie CowAgent up to 2.1.9. The impacted element is an unknown function of the component Media Download Handler. Such manipulation leads to uncontrolled memory allocation. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2.2.0 is sufficient to resolve this issue. The name of the patch is b7967210268fc4c0afea1078223e74e7e96a8a54. You should upgrade the affected component.	4.3	More Details
CVE-2026-108705	CordysCRM through 1.9.3 contains a missing authorization vulnerability in the POST /custom-form/data/import endpoint that allows authenticated users to import data into any custom form by customFormId. Low-privileged attackers can upload Excel files with importType ADD or UPDATE to create records in, or overwrite existing records of, custom forms they cannot manage.	4.3	More Details
CVE-2026-108704	CordysCRM through 1.9.3 contains an authorization bypass vulnerability that allows low-privileged authenticated users to skip permission checks by setting the owner field to their own user id. Attackers can send requests to the follow/record/add endpoints to add follow-up records and overwrite follow_time and follower on any known customer, clue or opportunity.	4.3	More Details
CVE-2026-108811	A weakness has been identified in WMCMS 4.446.1257. The affected element is an unknown function of the file /index.php. This manipulation of the argument path/file causes information disclosure. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-108702	1Panel-dev CordysCRM through 1.9.3 lacks a PROCESS_SETTING permission check on POST /approval-flow/webhook/test, allowing any authenticated user to trigger server-side requests to attacker-supplied URLs. Attackers can redirect GET requests from a controlled host to bypass SSRFValidator and probe internal addresses through success or failure results.	4.3	More Details
CVE-2026-108701	1Panel-dev CordysCRM before 1.9.2 contains a missing authorization vulnerability in the ContractController sortModule handler for POST /contract/sort, which lacks any permission annotation. Authenticated users without contract update permission can supply a dragNodeId, stage and field values to modify any contract, including contracts in other organizations.	4.3	More Details
CVE-2026-108696	CoreShop through 1.5.5 contains an authorization bypass vulnerability in the OrderController that allows authenticated customers to act on other customers' orders by supplying user-controlled ids. Attackers can omit the data field in OrderConfirm or supply another reshipId to SendReship to confirm receipt of others' orders and overwrite return tracking details.	4.3	More Details
CVE-2026-108730	Raven 2.0.0 through 3.0.0 contains a missing authorization vulnerability in legacy methods in raven/api/raven_message.py that skip the workspace membership check. Authenticated non-members can call get_messages_with_dates or get_all_files_shared_in_channel with predictable channel IDs to read Public channel history and Open/Public channel file metadata across workspaces.	4.3	More Details
CVE-2026-108796	A flaw has been found in ZKTeco BioTime 9.5.6 Build 20260130.3206. This affects an unknown part of the file /iclock/finger_data/ of the component Biometric Data Endpoint. Executing a manipulation of the argument emp_code can lead to authorization bypass. The attack can be launched remotely. The vendor was contacted	4.3	More Details

	early about this disclosure but did not respond in any way.		
CVE-2026-108663	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysTenantController deleteApply handler that allows any authenticated user to reject tenant administrator applications. Low-privileged attackers can send PUT requests with chosen tenantId, packId and userId values to delete pending applications in any tenant and notify applicants of rejection.	4.3	More Details
CVE-2026-108800	A vulnerability was identified in yangzongzhuan RuoYi 4.8.3. The affected element is an unknown function. Such manipulation leads to cross-site request forgery. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-106570	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32, an unauthenticated adjacent-network client can repeatedly connect to the distributed pixel cache server and exhaust its available connections, causing denial of service. This issue is fixed in version 7.1.2-32.	4.3	More Details
CVE-2026-84166	The Hotel Booking WordPress plugin through 3.8 does not implement CSRF protection on its administrative booking order management, allowing attackers to trick a logged-in administrator into creating, deleting, or modifying arbitrary booking order records via a forged request.	4.3	More Details
CVE-2026-108873	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to modify any department by calling PUT /sys/user/doUpdateDepartInfo. Attackers can supply a department id to rename or re-parent it and replace or remove its department heads without ownership or tenant checks.	4.3	More Details
CVE-2026-108872	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the batchEditUsers handler of SysUserController that allows any authenticated user to edit user department assignments. Low-privileged attackers can send PUT requests to /sys/user/batchEditUsers with arbitrary user and department ids to move users, including administrators, between departments and overwrite positions.	4.3	More Details
CVE-2026-108875	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysUserController addSysUserGroup handler that allows any authenticated user to modify user group membership. Low-privileged attackers can send POST requests with arbitrary user ids and a groupId to add any users to administrator-maintained groups without permission checks.	4.3	More Details
CVE-2026-108869	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to send system announcements by calling POST /sys/api/sendSysAnnouncement. Attackers can supply arbitrary title, content, fromUser and toUser values to deliver forged announcements to any users via WebSocket, WeCom, DingTalk and Feishu.	4.3	More Details
CVE-2026-108726	GLPI through 12.0.0 contains a missing authorization vulnerability in ajax/map.php that allows authenticated low-privileged users to search itemtypes they cannot view by omitting the canView() check. Attackers can submit crafted itemtype and search criteria for types like Contact, Supplier, Contract and Budget to obtain match counts, titles and coordinates within their entities.	4.3	More Details
CVE-2026-108797	A vulnerability has been found in ZKTeco BioTime 9.5.6 Build 20260130.3206. This vulnerability affects unknown code of the file /personnel/api/employees/ of the component Employee REST API. The manipulation leads to authorization bypass. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-78358	Several administrative actions do not sufficiently validate whether a request was intentionally initiated by the authenticated user. In particular, the DBUpdateLogCleanUp action can be triggered through a GET request without validating a ChallengeToken. An unauthenticated remote attacker can therefore cause the browser of an authenticated administrator to execute the cleanup action by embedding a crafted request in a malicious web page. Successful exploitation can delete existing DBUpdate log entries. This may reduce the availability of diagnostic and historical information used for troubleshooting and auditing. The impact is limited to DBUpdate log entries that exist at the time the forged request is processed. Additional administrative endpoints were identified that do not validate a ChallengeToken. Some of these endpoints can trigger administrative actions such as deploying or synchronizing already existing configuration. They do not allow an attacker to introduce arbitrary new configuration through the CSRF request itself. Export and read-only endpoints were also identified without ChallengeToken validation. While these endpoints may be triggered through a forged cross-site request, the response content remains subject to the browser's same-origin restrictions and is not automatically exposed to the attacker. Therefore, no direct confidentiality impact has been demonstrated for these endpoints. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.7.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	4.3	More Details
CVE-2026-108868	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to publish templated system announcements via POST /sys/api/sendBusTemplateAnnouncement. Low-privileged attackers can supply templateCode, toUser, and a forged fromUser to send notifications to arbitrary users through WebSocket, DingTalk, WeCom, Feishu and UniPush channels.	4.3	More Details
CVE-	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SystemApiController getUserRoleSetById handler that allows any authenticated user to read other users' role assignments. Low-		More

2026-108867	privileged attackers can supply an arbitrary userId parameter to retrieve assigned role codes and identify administrator accounts without the system:user:queryUserRole permission.	4.3	Details
CVE-2026-108727	EdgeEver through 1.108.0 contains a missing authorization vulnerability in the Hono API memo-template routes that allows holders of scoped API tokens to bypass token scope restrictions because template handlers never call requireScopes. Attackers with a token lacking write:memos can save a template and invoke POST /api/v1/templates/:id/use to create memos, and list, modify, or delete templates in the token owner's workspace.	4.3	More Details
CVE-2026-108866	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows authenticated users to read any account's permissions via the queryUserAuths handler. Low-privileged attackers can supply an arbitrary userId parameter to retrieve another user's complete permission set and identify administrator accounts.	4.3	More Details
CVE-2026-107429	Improper Validation of Specified Quantity in Input vulnerability in VideoWhisper.com Paid Videochat Turnkey Site ppv-live-webcams allows Input Data Manipulation.This issue affects Paid Videochat Turnkey Site: from n/a through 7.5.12.	4.3	More Details
CVE-2026-107423	Missing Authorization vulnerability in WP User Manager WP User Manager wp-user-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Manager: from n/a through 2.9.22.	4.3	More Details
CVE-2026-108876	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the putCancelQuit handler of SysUserController, allowing any authenticated user to cancel user resignations. Low-privileged attackers can supply user ids and a tenantId parameter or X-Tenant-Id header to restore ended, pending, or refused tenant memberships to normal.	4.3	More Details
CVE-2026-97331	The User Private Files WordPress plugin before 2.1.9 does not validate that a supplied user belongs to the document being operated on before returning that user's email address, allowing any authenticated user, such as a Subscriber, to obtain the email address of any registered account, including administrators.	4.3	More Details
CVE-2026-108880	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the PUT /sys/dict/editDictByLowAppId endpoint that allows any authenticated user to modify low-code application dictionaries. Attackers can supply a dictionary's low_app_id, obtained from GET /sys/dict/list, via the lowAppId parameter or X-Low-App-ID header to rename dictionaries and replace their items.	4.3	More Details
CVE-2026-108669	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the embeddingSearch handler of AiragKnowledgeController that lacks Shiro permission annotations. Low-privileged authenticated attackers can supply knowledge base ids to the GET /airag/knowledge/embedding/search endpoint to read document text chunks from unauthorized knowledge bases.	4.3	More Details
CVE-2026-108750	OpenDocMan 2.4.0 through 2.10.0 contains a decompression bomb vulnerability that allows authenticated users to exhaust PHP memory by uploading crafted office documents. Attackers can upload a small ODT, DOCX, or XLSX file whose XML entries decompress to hundreds of megabytes, crashing PHP workers and degrading availability.	4.3	More Details
CVE-2026-104651	The Yaad Sarig Payment Gateway For WC WordPress plugin before 2.2.13 does not verify authorization or that the requesting user owns the target order in several of its order payment-processing actions, allowing any authenticated user, including subscribers, to act on and alter orders belonging to other customers.	4.3	More Details
CVE-2026-104050	The Academy LMS WordPress plugin before 4.0.0 does not verify that a quiz question belongs to the course the requesting user is authorized to access before returning that question's answer options, allowing any authenticated user with access to a single course, such as an enrolled student, to read the quiz answer options of questions belonging to other courses they are not enrolled in.	4.3	More Details
CVE-2026-108667	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to restore deleted AI prompt templates by calling the revertRecycleBin endpoint. Attackers can send PUT requests to /airag/prompts/revertRecycleBin with chosen template ids to clear deleted flags, undoing administrator removals.	4.3	More Details
CVE-2026-104049	The Academy LMS WordPress plugin before 4.0.0 does not verify course enrollment or object ownership when returning a lesson's content through one of its REST API routes, allowing users with a self-registerable student account to read the full content of arbitrary lessons, including lessons of paid or private courses they are not enrolled in.	4.3	More Details
CVE-2026-103075	Missing Authorization vulnerability in WPMU DEV Hustle wordpress-popup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hustle: from n/a through 7.8.14.2.	4.3	More Details
CVE-2026-108891	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysUserController getUserDetailByUserId handler that allows any authenticated user to read other users' details. Low-privileged attackers can supply arbitrary userId values to retrieve real names, usernames, emails, phone numbers, birthdays, employee numbers, department paths and posts.	4.3	More Details

CVE-2026-103681	The Frontend Dashboard WordPress plugin before 3.0.0 does not perform a capability check in one of its AJAX actions, allowing authenticated users with low privileges, such as subscribers, to delete the Frontend Dashboard WordPress plugin before 3.0.0's configured profile and post form fields.	4.3	More Details
CVE-2026-84167	The Hotel Booking WordPress plugin through 3.8 does not verify that a booking record belongs to the user requesting it, allowing any authenticated user such as a Subscriber to read other customers' booking details, including their name, email address, phone number and postal address, by referencing an identifier they do not own.	4.3	More Details
CVE-2026-108665	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragPromptsController edit handler that allows any authenticated user to modify AI prompt templates. Low-privileged attackers can send PUT or POST requests to /airag/prompts/edit with a template id to overwrite prompt text and model parameters created by administrators or other users.	4.3	More Details
CVE-2026-94235	The MemberHero WordPress plugin through 6.9 does not perform any capability or nonce check on one of its AJAX actions, allowing any authenticated user, such as a subscriber, to make the site send arbitrary HTML emails to arbitrary recipients from its own mail system, which can be abused to relay phishing carrying the site's identity and domain reputation.	4.3	More Details
CVE-2026-108720	phpIPAM through 1.8.3 contains a missing authorization vulnerability that allows authenticated low-privilege users to view restricted subnets and addresses because customer, location and NAT pages skip Subnets::check_permission. Attackers can open customer objects.php, single-location.php or nat_details.php to read IP addresses, CIDRs, hostnames and MAC addresses from sections they cannot access.	4.3	More Details
CVE-2026-108664	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragPromptsController queryById handler that allows low-privileged authenticated users to read any AI prompt template. Attackers can enumerate ids via the unguarded /airag/prompts/list endpoint and query each one to obtain prompt text, model parameters, and creator details belonging to administrators or other users.	4.3	More Details
CVE-2026-108670	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the promptExperiment handler of AiragPromptsController that allows any authenticated user to run AI prompt experiments. Low-privileged attackers can supply other users' prompt template and dataset ids to trigger large language model evaluation runs, write result rows into airag_ext_data, and change dataset status.	4.3	More Details
CVE-2026-108672	JeecgBoot through 3.9.5 contains an authorization bypass vulnerability in the getVideoRecords handler of VideoGenerationController that allows authenticated users to read other users' records via the userId parameter. Low-privileged attackers can supply another user id to retrieve their AI video generation history, including prompts, task ids, video URLs and cover URLs.	4.3	More Details
CVE-2026-108673	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragPromptsController exportXls handler that allows any authenticated user to export all AI prompts. Low-privileged attackers can request /airag/prompts/exportXls to download every user's prompts, including prompt content, model ids, and parameters, as an Excel workbook.	4.3	More Details
CVE-2026-108674	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the OpenApiController queryById handler that allows low-privileged authenticated users to read OpenAPI definitions without openapi permissions. Attackers can request GET /openapi/queryById with an entry id to obtain internal origin URLs, virtual paths, IP whitelists, and header and parameter templates.	4.3	More Details
CVE-2026-108675	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysAnnouncementController editTop handler that allows low-privileged authenticated users to change announcement pin status. Attackers can send POST or PUT requests with any announcement id to pin or unpin system notices shown at the top for all users.	4.3	More Details
CVE-2026-108676	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysAnnouncementController downloadFiles handler that allows low-privileged authenticated users to download announcement attachments. Attackers can supply a known announcement id to retrieve a ZIP of attachments from unreleased announcements or those addressed only to other users.	4.3	More Details
CVE-2026-108879	JeecgBoot through 3.9.5 contains an insecure direct object reference vulnerability in AiragBaseApiController that allows authenticated users to read other users' AI chat variables via the username parameter. Attackers can send POST requests to /airag/api/getChatVariable with a target apId, username, and variable name to retrieve stored chat memory values from Redis.	4.3	More Details
CVE-2026-108861	Odoo MCP 1.0.0 through 1.3.2 contains an information disclosure vulnerability that allows MCP clients to bypass the field-level ACL by invoking the execute_method tool. Attackers or prompt-injected agents can call read or search_read through execute_method naming denied fields to receive their values unredacted.	4.3	More Details
CVE-2026-108678	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the queryUserRoles handler of SystemApiController that lets authenticated users read any user's role codes. Low-privileged attackers can send GET requests to /sys/api/queryUserRoles with an arbitrary username to enumerate role assignments and identify administrator accounts.	4.3	More Details

CVE-2026-108679	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the sendBusAnnouncement handler of SystemApiController that allows any authenticated user to send announcements without the required permissions. Low-privileged attackers can POST crafted bodies to /sys/api/sendBusAnnouncement with forged sender, recipients, title and content to deliver spoofed admin or system messages for phishing.	4.3	More Details
CVE-2026-108680	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows any authenticated user to send template notifications by calling POST /sys/api/sendTemplateAnnouncement. Low-privileged attackers can supply forged sender, recipients, title, and template parameters to deliver messages appearing to come from admin or system accounts.	4.3	More Details
CVE-2026-108688	Eladmin through 2.7 contains a missing authorization vulnerability in the LocalStorageController uploadPicture handler that allows low-privileged authenticated users to bypass the storage:add permission. Attackers can send POST requests with image-named files to /api/localStorage/pictures to write files into server local storage and disclose absolute server paths.	4.3	More Details
CVE-2026-108742	CloudBeaver through 25.3.5 contains a missing authorization vulnerability in the initConnection GraphQL mutation that lets view-only shared-project members persist credentials without datasource-edit permission. Attackers can set saveCredentials and sharedCredentials flags with chosen authProperties so other users connect to the shared connection under the attacker's database identity.	4.3	More Details
CVE-2026-108690	mall4j through 4.0 contains an information disclosure vulnerability that allows authenticated customers to read other shoppers' cart items due to an operator precedence error in the getShopCartExpiryItems SQL filter. Attackers with any storefront account can request GET /p/shopCart/expiryProdList to retrieve off-shelf product basket entries including product, SKU, quantity, shop, and promoter card numbers.	4.3	More Details
CVE-2026-107869	Missing Authorization vulnerability in WP Desk Flexible Subscriptions flexible-subscriptions allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flexible Subscriptions: from n/a through 1.8.4.	4.3	More Details
CVE-2026-108878	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragApiController queryById handler that allows low-privileged authenticated users to read any AI application configuration. Attackers can enumerate application ids via the unguarded /airag/app/listDict endpoint and query each id to obtain system prompts, memory prompts, model ids, knowledge base ids, and plugin bindings of other users' applications.	4.3	More Details
CVE-2026-108735	Miniflux 2.3.0 through 2.3.3 contains a server-side request forgery vulnerability that allows authenticated users to reach internal addresses by setting a feed's proxy_url. Attackers can point proxy_url at loopback or internal hosts, bypassing FETCHER_ALLOW_PRIVATE_NETWORKS checks to probe internal ports and send proxy-style requests to internal services.	4.3	More Details
CVE-2026-108734	Frappe CRM 1.49.0 through 1.87.0 contains a missing authorization vulnerability in crm.api.doc.get_linked_docs_of_document that allows authenticated users to read linked documents without permission checks. Attackers can name a lead, deal, comment or user they cannot read to obtain linked call log phone numbers, deal organizations and mention notification text.	4.3	More Details
CVE-2026-105275	Satel Netco Design versions prior to v2.1.7 contains a relative path traversal vulnerability in its data import functionality. An authenticated user with Viewer privileges could access file paths outside the intended directory and use observable application responses to determine whether files exist on the host system.	4.3	More Details
CVE-2026-108625	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to modify message push records by calling PUT /sys/message/sysMessage/edit. Attackers can submit a request body naming any sys_sms record id to overwrite its title, content, receiver address and send status without ownership checks.	4.3	More Details
CVE-2026-91050	The Appointment Booking Plugin – LatePoint Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference / Missing Authorization in versions up to, and including, 5.7.2. This is due to the publicly reachable steps__start and steps__load_step routes accepting a params[presets][order_item_id] value that is copied verbatim into the booking object without verifying that the referenced order item belongs to the current customer, is a bundle item, is paid, or has remaining capacity — the is_bundle_scheduling() bundle discriminator is a mere !empty(order_item_id) truthiness check, and the code flow explicitly removes the customer and payment steps when this is truthy (the source even carries a TODO acknowledging the missing validation). This makes it possible for unauthenticated attackers to create approved appointments against other customers' order items and to read those customers' names, email addresses, and order codes returned in the booking confirmation.	4.3	More Details
CVE-2026-105831	EspoCRM before 10.0.6 contains a stored HTML injection vulnerability that allows unauthenticated attackers to inject HTML by submitting crafted Lead Capture public form data. The request body is stored in LeadCaptureLogRecord.data and rendered unescaped when administrators view the log record, though Content Security Policy blocks JavaScript execution.	4.3	More Details
CVE-2026-108621	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the SysPositionController edit handler that allows any authenticated user to modify organizational positions. Low-privileged attackers can obtain position ids from the unguarded list endpoint and send PUT or POST requests to /sys/position/edit to	4.3	More Details

	alter position names, codes, and ranks.		
CVE-2026-108111	ruoyi-ai 3.0.0 through 3.1.0 contains a missing authorization vulnerability in the GET /workflow/search endpoint that exposes other users' private workflows. Authenticated non-admin users can query this endpoint, which lacks owner or is_public filtering, to list enabled private workflows in the same tenant, including UUIDs and full node and edge configurations.	4.3	More Details
CVE-2026-105891	Missing Authorization vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through 5.30.0.1.	4.3	More Details
CVE-2026-103072	Missing Authorization vulnerability in VillaTheme VillaTheme Core villatheme-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VillaTheme Core: from n/a through 1.0.5.	4.3	More Details
CVE-2026-107850	Contao is an Open Source CMS. From version 5.7.1 until 5.7.12, core-bundle/config/services.yaml registers the preview access voter as Contao\CoreBundle\Security\Voter\DataContainer\PreviewAccessVoter although the shipped class is PreviewVoter. Symfony therefore omits voter autoconfiguration and removes the private service, so PreviewVoter::hasAccess() never enforces ownership. A non-admin backend user with the preview_link module can list every tl_preview_link record, obtain signed share URLs created by other users, and use them to view unpublished pages with showUnpublished despite lacking page permission. The advisory does not establish editing or deletion of foreign links. This issue is fixed in version 5.7.12.	4.3	More Details
CVE-2026-107851	Contao is an Open Source CMS. From version 5.7.0 until 5.7.12, TableAccessVoter::hasAccessToModule() in core-bundle/src/Security/Voter/DataContainer/TableAccessVoter.php caches authorization decisions using only \$tokenHash, a hash of the user's security token, and omits the table returned by getDataSource(). If one request first checks a table allowed to the user and then a different denied table, the voter can reuse the allowed result, while DefaultDataContainerVoter can convert an incorrect abstention into a grant. A low-privileged backend user can consequently read, create, update, or delete records in tables outside assigned module permissions, including tables containing member or newsletter-subscriber data. This issue is fixed in version 5.7.12.	4.3	More Details
CVE-2026-103964	The Download Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.71 via the 'first_name' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the administrator's full Cookie header, including wordpress_logged_in_* session cookies, from the suspension email sent during the administrator's authenticated request, enabling full session hijack and account takeover. Exploitation requires an administrator to perform the Suspend action against the attacker's account, which causes the plugin to synchronously compile and send the suspension email inside the administrator's authenticated HTTP request — making the administrator's session cookies available to the template engine at send time.	4.3	More Details
CVE-2026-94244	The Wallet System for WooCommerce WordPress plugin before 2.8.0 does not perform any capability check, and relies on a token any authenticated user can obtain from a front-end page, before generating a report containing every customer's wallet transaction history, allowing any authenticated user, such as a subscriber, to disclose all users' names, email addresses, roles, transaction amounts, payment methods and dates.	4.3	More Details
CVE-2026-87669	A missing authorization check in Brocade Fabric OS versions before 10.0.1 REST API interface of affected platform releases allows an authenticated user, regardless of their assigned role or administrative scope, to retrieve complete Monitoring and Alerting Policy Suite (MAPS) violation data across all logical switches. An attacker with low-privilege API access can leverage this endpoint to dump chassis-wide system health metrics, port performance violations, and configuration data without appropriate privileges.	4.3	More Details
CVE-2026-105260	The Database Addon For WPForms (wpforms entries) WordPress plugin before 1.1.1 does not verify the CSRF nonce when the field is omitted and performs no capability check of its own, allowing attackers to delete arbitrary stored form entries by tricking a logged-in administrator into loading a crafted page.	4.3	More Details
CVE-2026-104728	The AutomatorWP – No-Code Workflow Automation, Integration & Webhooks Plugin, now with AI plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.8.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to enumerate all Fluent Forms records, including form IDs and titles, from the fluentform_forms database table.	4.3	More Details
CVE-2026-105194	The Easy Digital Downloads WordPress plugin before 3.7.1 does not restrict a block's order data to the current user, allowing users with subscriber-level access to view other customers' recent order products and obtain signed download links that grant access to paid digital files without purchase.	4.3	More Details
CVE-2026-108165	Immich through 3.3.1 contains a missing authorization vulnerability in the partner synchronization stream that allows authenticated partners to read Locked Folder asset metadata because sync queries do not exclude Locked visibility. Attackers with an active partner relationship can call POST /api/sync/stream with PartnerAssetsV2 and PartnerAssetExifsV1 types to obtain GPS coordinates, capture times, descriptions and camera details.	4.3	More Details
	Strapi 5.47.0 through 5.57.0 contains an improper authorization vulnerability that allows admin API tokens to		

CVE-2026-108114	retain all-field Content Manager access after the owner's role is field-restricted. Because reconcileTokenPermissionsToUserCeiling ignores token permissions with omitted or null fields, token holders can keep reading content fields an administrator removed from the role.	4.3	More Details
CVE-2026-107444	A flaw was found in Katello where the Docker Tags repositories API does not properly enforce organization scoping when listing repositories for a Docker meta tag. An authenticated user with permission to view products in one organization may be able to retrieve repository metadata associated with Docker tags belonging to another organization by supplying the tag identifier. This can result in unauthorized disclosure of repository configuration information across organization boundaries.	4.3	More Details
CVE-2026-103685	Missing Authorization vulnerability in VillaTheme ALD - Dropshipping and Fulfillment for AliExpress and WooCommerce woo-alidropship allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ALD - Dropshipping and Fulfillment for AliExpress and WooCommerce: from n/a through 2.2.4.	4.3	More Details
CVE-2026-108602	Helicone through v2025.08.21-1 contains a server-side request forgery vulnerability in the Jawn webhook sender that allows authenticated organization users to reach internal services by using hostnames resolving to private addresses. Attackers can create webhooks with public hostnames that resolve or DNS-rebind to loopback or internal addresses, causing blind POST requests to internal HTTPS services.	4.3	More Details
CVE-2026-105832	EspoCRM before 10.0.6 contains an authentication bypass vulnerability that accepts a login stopped at the second factor on routes not requiring authentication. Attackers knowing a 2FA-enabled user's username and password can skip the second factor to read config parameters not exposed publicly.	4.3	More Details
CVE-2026-101022	A Modbus connection feature on openPDC accepts a caller-specified destination address and port with no restriction on which internal hosts may be targeted. An authenticated user can attempt connections to arbitrary internal network destinations, revealing which destinations are reachable. With repeated attempts, an attacker may be able to map the internal network.	4.3	More Details
CVE-2026-107586	Uncontrolled eviction in the browser session table of the REST API in Progressive Robot hMailServer 6.2.28 through 6.3.5 allows a remote authenticated user to end other users' sessions. The table of browser sessions, shared by every account, the server administrator and support sessions, dropped its least recently used session whenever it was full, whoever it belonged to, and placed no limit on how many sessions one account could hold. A user who repeatedly signs in with their own mailbox password can therefore keep the table full and sign out every webmail and administration session that is idle for more than a short time, for as long as they continue.	4.3	More Details
CVE-2026-107623	A flaw was found in the OIDC Dynamic Client Registration (DCR) component of Keycloak. A bug in the response serialization causes the backchannel logout offline token revocation setting to be omitted from responses. When a client performs a standard update, this missing information causes the setting to be silently disabled. As a result, offline tokens may remain valid even after a user session is terminated via backchannel logout.	4.3	More Details
CVE-2026-78388	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	4.3	More Details
CVE-2026-107792	Jivejdon from commit d58a36b0 through commit ee67a65e contains a missing authorization vulnerability in UpdateThreadToForumAction that allows authenticated users to move other users' threads. Attackers can send crafted threadId and forumId values to /message/threadToForum/save to relocate any reply-less thread into an arbitrary forum.	4.3	More Details
CVE-2026-107793	Jivejdon through 5.0 contains an authorization bypass vulnerability in SubscriptionServiceImp.deleteSubscription that allows authenticated users to delete other users' subscriptions by ID. Attackers can submit a delete action to /account/protected/sub/subSaveAction with another user's subscriptionId to remove their thread, forum, tag or account subscriptions.	4.3	More Details
CVE-2026-107831	Jivejdon through 5.0 contains a cross-site request forgery vulnerability that allows remote attackers to perform state-changing actions by abusing GET endpoints lacking anti-CSRF tokens. Attackers can lure authenticated users to crafted links targeting /account/protected/delAll, /account/protected/sub/delSub, or /message/updateAction to delete private messages and subscriptions or rename threads.	4.3	More Details
CVE-2026-107706	Dolibarr ERP CRM before 24.0.2 contains an incorrect authorization vulnerability in htdocs/core/ajax/updateextrafield.php that checks only read permission before writing extrafield values. Authenticated users with read-only access can POST objectType, objectId, field and value parameters to persistently modify extrafields on viewable third parties, products, members, projects or contacts.	4.3	More Details
CVE-2026-107395	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to 3.3.13, an authenticated user can misuse the legacy session export API to retrieve details for a restricted session without access to that session, as long as the containing event is accessible. The missing access check can disclose session metadata such as the title, description, and conveners. This issue is fixed in version 3.3.13.	4.3	More Details

CVE-2026-92989	The SendPress Newsletters WordPress plugin through 1.26.1.20 does not check the user's capability on several newsletter-management actions, allowing any authenticated subscriber-level user to synchronise all site users into a mailing list and to drive the newsletter send queue.	4.3	More Details
CVE-2026-106434	The explicit decryption component of MongoDB libmongocrypt can return an unrecognized encrypted payload unchanged instead of returning a decryption error. An actor who can modify stored encrypted fields, such as a database writer, server, or network intermediary, can cause an affected application to process the supplied bytes as decrypted plaintext.	4.3	More Details
CVE-2026-76769	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	4.3	More Details
CVE-2026-78026	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Authorization Bypass Through User-Controlled Key vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	4.3	More Details
CVE-2026-107702	QloApps through 1.7.0 contains an authorization bypass vulnerability in AdminHotelRoomsBookingController::postProcess() that allows restricted back-office employees to access other hotels' data by supplying an id_hotel parameter. Attackers can modify the id_hotel URL parameter on the Book Now page to view room availability and booking status of hotels outside their assigned profile access.	4.3	More Details
CVE-2026-107697	FFmpeg before 8.1.3 contains a protection mechanism failure in the HLS demuxer that allows attackers to bypass protocol and allowed_extensions restrictions when opening child playlists. Attackers can supply a crafted master playlist whose child playlists use disallowed protocols or non-multimedia local files, making parse_playlist() open resources the HLS security policy should block.	4.3	More Details
CVE-2026-107291	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 0.3.4 until 1.107.6 and 2.44.0, OpenTelemetry instrumentation configured with InstrumentationSettings(include_content=False) can still export sensitive agent content through exception.message and exception.stacktrace events, error status descriptions, and model_request_parameters containing instructions or the prompted_output_template. The exposed data is available to readers of the configured telemetry backend and can include tool feedback, provider error bodies, runtime instructions, and structured-output templates even though message attributes are redacted. This issue does not grant new access to agent data, and deployments that do not use include_content=False are not affected by the setting bypass. This issue is fixed in versions 1.107.6 and 2.44.0.	4.3	More Details
CVE-2026-39779	Missing Authorization vulnerability in Asgaros Asgaros Forum asgaros-forum allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Asgaros Forum: from n/a through 3.4.0.	4.3	More Details
CVE-2026-85348	The GDPR Data Request Form WordPress plugin through 1.7.1 does not have CSRF protection when updating one of its settings, allowing attackers to change that setting 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-2026-104079	Envira Gallery Lite before 1.16.2 contains a missing authorization vulnerability in its gallery conversion REST endpoint that allows lower-privileged authenticated users to create and publish Envira galleries without the required capabilities, because the endpoint only checks edit permissions on the source post and uses a hard-coded publish status. Attackers can also supply arbitrary caller-controlled image IDs without ownership verification to publish unauthorized content using attachments they are not authorized to use.	4.3	More Details
CVE-2026-107637	pH7Builder (pH7 Social Dating CMS) before 18.5.0 contains an improper authorization vulnerability in the note module delete() action that allows authenticated members to delete other members' note comments and categories. Attackers can submit another member's note ID in the POST id parameter to remove all comments and category associations, since those queries lack profile ID checks.	4.3	More Details
CVE-2026-87670	An authorization logic vulnerability exists in the Brocade Fabric OS versions before 10.0.1 REST API gateway. The internal gate guarding restricted management endpoints relies exclusively on client-controlled HTTP headers. An authenticated user with any valid REST session can spoof these headers to gain unauthorized access to internal management endpoints. This allows low-privilege users to view sensitive chassis metadata, hardware memory patrolling state, and firmware integrity audit logs.	4.3	More Details
CVE-2026-62036	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in AREOI All Bootstrap Blocks all-bootstrap-blocks allows Retrieve Embedded Sensitive Data.This issue affects All Bootstrap Blocks: from n/a through 1.3.31.	4.3	More Details
CVE-2026-	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the edit_spl2_module_permissions capability could use the affected Representational State Transfer (REST) API to access permission grants for SPL2 modules that the user does not have permission to view. The vulnerability is possible because Splunk Enterprise does not verify that the user can read the requested app before the affected REST API returns SPL2 module permission grants. For more information see Module permissions	4.3	More Details

76278	(https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/modules-statements-and-views/module-permissions) and Manage SPL2 modules (https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/multiple-searches-in-an-spl2-module/manage-spl2-modules) in the Splunk documentation. Splunk Enterprise versions 9.4.x are not affected.		
CVE-2026-108614	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiragExtDataController exportXls handler that allows any authenticated user to export AI evaluator data. Low-privileged attackers can request /airag/extData/exportXls to download every user's airag_ext_data evaluator definitions and test-tracking records as an Excel workbook.	4.3	More Details
CVE-2026-108608	JeecgBoot through 3.9.5 contains an insecure direct object reference vulnerability that allows authenticated users to delete other users' AI voice records by supplying an arbitrary userId to DELETE /airag/voice/deleteVoiceRecord. Attackers can obtain record ids from the unchecked GET /airag/voice/listByUser endpoint and delete victims' text-to-speech history entries stored in Redis, one per request.	4.3	More Details
CVE-2026-108607	JeecgBoot through 3.9.5 contains an insecure direct object reference vulnerability that allows authenticated users to delete other users' AI video generation records by supplying arbitrary userId values to DELETE /airag/video/deleteVideoRecord. Attackers can obtain record ids from the unchecked GET /airag/video/listByUser endpoint and delete victims' Redis-stored video history entries one record per request.	4.3	More Details
CVE-2026-108605	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AiOcrController updateByld handler that allows any authenticated user to modify global OCR templates. Low-privileged attackers can send PUT requests to /airag/ocr/edit to overwrite LLM prompts in the shared airag:ocr Redis key, corrupting OCR results for all users.	4.3	More Details
CVE-2026-76279	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the run_collect capability could use the collect Search Processing Language (SPL) command to write events to internal indexes outside the index access configured for the role. The vulnerability is possible because Splunk Enterprise does not normalize whitespace in an index name before applying configured index-access restrictions for the role. For more information see collect (https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.4/search-commands/collect), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and How indexing works (https://help.splunk.com/en/splunk-enterprise/administer/manage-indexers-and-indexer-clusters/10.4/indexing-overview/how-indexing-works) in the Splunk documentation.	4.3	More Details
CVE-2026-76276	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a low-privileged user that does not hold the "admin" or "power" Splunk roles could retrieve original source code for the Discover Splunk Observability Cloud app through Splunk Web. The vulnerability is possible because production JavaScript bundles for the app contain embedded source maps that include original source code. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access), Splunk Observability Cloud previews (https://help.splunk.com/en/splunk-enterprise/search/search-manual/10.4/observability/splunk-observability-cloud-previews), and Navigating Splunk Web (https://help.splunk.com/en/splunk-enterprise/search/search-tutorial/10.4/part-1-getting-started/navigating-splunk-web) in the Splunk documentation. Splunk Enterprise versions 9.4.x are not affected.	4.3	More Details
CVE-2026-76275	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the "admin" or "power" Splunk roles could access search query text and job metadata for jobs that belong to other users, including job identifiers, dispatch parameters, result counts, and execution metadata, through an Application Programming Interface (API) implemented as a Representational State Transfer (REST) API. The vulnerability is possible because the REST API does not fully enforce per-user authorization before it includes job information in search job listings.	4.3	More Details
CVE-2026-76273	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the run_collect capability could use the collect Search Processing Language (SPL) command to add attacker-controlled content to system-level messages on the Splunk platform instance. The vulnerability is possible because the collect command does not validate the index name before processing the value. For more information see collect (https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.4/search-commands/collect), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and System endpoint descriptions (https://help.splunk.com/en/splunk-enterprise/rest-api-reference/10.4/system-endpoints/system-endpoint-descriptions) in the Splunk documentation.	4.3	More Details
CVE-2026-108610	JeecgBoot through 3.9.5 contains a missing authorization vulnerability in the AigcWordTemplateController edit handler that allows any authenticated user to modify word templates. Low-privileged attackers can send PUT or POST requests to /airag/word/edit to overwrite shared templates that other users rely on to generate documents.	4.3	More Details
	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the "admin"		

CVE-2026-76272	or "power" Splunk roles could cause Splunk Secure Gateway to sign attacker-controlled payloads. The vulnerability is possible because Splunk Secure Gateway does not verify that the user is authorized to request a signature. Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72 are also affected. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	4.3	More Details
CVE-2026-108609	JeecgBoot through 3.9.5 contains an insecure direct object reference vulnerability that allows authenticated users to read other users' AI voice generation history via the userId parameter of GET /airag/voice/listByUser. Attackers who know another user's id can retrieve submitted text-to-speech input, voice settings, timestamps, and generated audio file names and paths stored in Redis.	4.3	More Details
CVE-2026-76267	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the read_o11y_content capability could inject forged entries into the app log through the Representational State Transfer (REST) API. The vulnerability is possible because Splunk App for Splunk O11y Cloud does not neutralize user-supplied SignalFlow content before writing it to the app log. Splunk Enterprise versions 9.4.x are not affected.	4.3	More Details
CVE-2026-76264	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.10, and 9.4.15, a user who does not hold the "admin" or "power" Splunk roles could create or edit scripted lookup definitions through raw configuration endpoints. The vulnerability is possible because raw transforms configuration write paths do not apply external lookup capability checks before saving scripted lookup settings.	4.3	More Details
CVE-2026-108618	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to modify message templates via PUT /sys/message/sysMessageTemplate/edit. Attackers can obtain template ids from the unguarded list endpoint and overwrite system notification titles and content, delivering attacker-supplied text or links to other users.	4.3	More Details
CVE-2026-108617	JeecgBoot through 3.9.5 contains a missing authorization vulnerability that allows low-privileged authenticated users to create message templates by calling POST /sys/message/sysMessageTemplate/add. Attackers holding only minimal roles can insert arbitrary notification templates with chosen codes and content into the shared sys_sms_template library used for system, e-mail, SMS and IM notifications.	4.3	More Details
CVE-2026-108864	iFlytek Astron Agent through 1.1.2 contains an insecure direct object reference vulnerability that allows authenticated applications to resume other applications' paused workflows by supplying their event_id to POST /workflow/v1/resume. Attackers can predict Snowflake event IDs to inject resume content into victim workflows and read their continuation output stream, breaking cross-tenant isolation.	4.2	More Details
CVE-2026-108583	zotero-mcp 0.10.0 through 0.14.1 contains a server-side request forgery vulnerability that allows attackers to reach internal services because _fetch_embedded_metadata fetches URLs without destination validation. Attackers can steer the agent via prompt injection into calling zotero_add_by_url, causing requests to loopback, private, or link-local hosts directly or via redirects, leaking citation meta-tags and error details.	4.2	More Details
CVE-2026-108830	A weakness has been identified in meetecho janus-gateway up to 1.4.2. This affects an unknown part of the file src/plugins/janus_videoroom.c of the component VideoRoom. This manipulation causes race condition. Remote exploitation of the attack is possible. The attack's complexity is rated as high. It is indicated that the exploitability is difficult. The exploit has been made available to the public and could be used for attacks. Patch name: 27c0d1af888153e818675b56a4e6267f62d57097. Applying a patch is the recommended action to fix this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	4.2	More Details
CVE-2026-107719	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.3.4, the fast-jwt createVerifier cache can continue accepting a previously valid, signed JWT after its exp time when caching is enabled and the token has exp but no iat. In src/verifier.js, cacheSet derives the exp cache deadline only when iat is present, so the cache falls back to cacheTTL, and a later cache hit returns the saved payload before verifyToken rechecks expiration. An attacker who can replay the same cached bearer token can extend access until the cache entry expires, but cannot forge a token through this issue. This issue is fixed in version 6.3.4.	4.2	More Details
CVE-2026-107361	The Arkime live capture service (arkime-live) in Malcolm runs with network_mode: host, exposing port 8005 on all network interfaces (viewHost=0.0.0.0). Arkime trusts the X-Forwarded-User header from any IP address (userAuthlps=::,0.0.0.0/0) and auto-creates users with full access. The passwordSecret is hardcoded to the public value "Malcolm". A network-adjacent attacker bypasses nginx entirely by connecting directly to port 8005 with a forged identity header.	4.2	More Details
CVE-2026-108722	open-computer-use through commit 610bac8 contains a stored cross-site scripting vulnerability in Logger.write_log_file in os_computer_use/logging.py, which writes transcript text into log.html without HTML escaping. Attackers controlling sandbox content, such as web pages or files appearing in run_command output, can inject script that runs when operators open the log, exfiltrating transcript contents.	4.2	More Details
CVE-2026-108738	Traccar 5.7 through 6.16.0 contains a cross-site request forgery vulnerability that allows attackers to log victims into attacker-controlled accounts because the OpenID Connect callback never validates the OAuth state parameter. Attackers can induce a victim's browser to load /api/session/openid/callback with their own authorization code, causing data the victim enters, such as registered devices, to land in the attacker's	4.2	More Details

	account.		
CVE-2026-108555	PairDrop through 1.11.2 contains an IP spoofing vulnerability in Peer._setIP that allows remote attackers to join other networks' discovery rooms by supplying a forged cf-connecting-ip header. Attackers who know a victim's public IP can appear as a local device on self-hosted instances not behind Cloudflare to send or receive files.	4.2	More Details
CVE-2026-108747	Lightdash through 2.556.0 contains an authorization bypass vulnerability that allows authenticated organization members to delete other users' personal access tokens by supplying their UUID. Attackers can send DELETE requests to the personal-access-tokens route with a victim's token UUID, even across organizations, to revoke it and break API integrations.	4.2	More Details
CVE-2026-108579	OpenPanel through 2.3.0 contains a CSV formula injection vulnerability that allows unauthenticated attackers to embed spreadsheet formulas by supplying crafted profile IDs to the /track endpoint. Attackers can send tracking events with profile IDs like =HYPERLINK(...) matching a cohort, so exported cohort CSVs execute formulas that exfiltrate adjacent cell data.	4.2	More Details
CVE-2026-108752	JupyterHub through 6.0.1 contains an identifier collision vulnerability that allows authenticated users to overwrite another user's named-server OAuth client by registering a hyphenated username. Attackers holding a name like alice-prod can overwrite the client for alice's server prod, breaking OAuth login and revoking tokens by stopping their own server.	4.2	More Details
CVE-2026-108856	UnicomAI Wanwu through 0.6.5 contains an authorization bypass vulnerability that allows authenticated users to mint AppKeys bound to other users' MCP servers via POST /v1/appspace/app/key. Attackers supplying a victim's MCP server UUID with appType mcpserver can open MCP sessions and invoke the server's tools using the victim's upstream authentication.	4.2	More Details
CVE-2026-105140	Obot 0.25.0 before 0.25.6 and 0.26.0 before 0.26.1 contains a race condition in auth provider group refreshes that can restore group memberships just revoked in the identity provider. When overlapping refreshes for the same user commit out of order, stale memberships are persisted and the user retains revoked group-based access for about ten minutes.	4.2	More Details
CVE-2026-108839	thClaws through 0.141.0 contains a link-following vulnerability in the post_inputs handler of the v1 API POST /v1/inputs endpoint that allows writes outside the workspace by following symlinks. Attackers who plant a symlink under the allowed inputs/ prefix can cause later authenticated uploads to write or truncate files outside the workspace with daemon privileges.	4.2	More Details
CVE-2026-107313	pgjdbc, the PostgreSQL JDBC Driver, versions 42.7.4 and 42.7.5 can send the previous contents of the GSS send buffer in place of the first part of a value on a connection with GSS encryption (gssEncMode=prefer or require), and the server stores the value without an error. The buffer is 16320 bytes with MIT Kerberos. The stored value then holds bytes of the messages the driver sent just before it on the same connection, such as the statement's SQL text, its other parameters, and earlier rows of the same batch, instead of the bytes the application supplied. Values at least as long as the buffer are affected when the driver writes them from a byte array: bind parameters set with setString, setBytes, or a BufferedWriter, CopyIn.writeToCopy, and LargeObject.write. Most such writes fail with an ArrayIndexOutOfBoundsException instead. The default, gssEncMode=allow, does not start GSS encryption, and connections without GSS encryption are not affected. Versions 42.7.3 and earlier are not affected, and 42.7.6 fixes the problem.	4.2	More Details
CVE-2026-104753	The Rank Math SEO WordPress plugin before 1.0.280 does not properly sanitise and escape a parameter before using it in a SQL query, allowing high-privilege users such as administrators to perform SQL injection attacks.	4.1	More Details
CVE-2026-108828	A vulnerability was identified in Zen Cart 2.2.2. Affected by this vulnerability is the function eval of the file admin/configuration.php of the component Admin Panel. The manipulation of the argument glID leads to sql injection. The attack may be initiated remotely. The attack is considered to have high complexity. The exploitation appears to be difficult. The exploit is publicly available and might be used. The vendor explains: "`set_function`/'use_function` are not editable through any normal admin UI (only at plugin-install time via SQL, or via direct database access)".	4.1	More Details
CVE-2026-108827	A vulnerability was determined in Zen Cart up to 2.2.2. Affected is the function zen_call_function of the file admin/includes/functions/general.php of the component Administrative Module Management. Executing a manipulation of the argument use_function can lead to code injection. The attack can be launched remotely. Attacks of this nature are highly complex. The exploitability is told to be difficult. The exploit has been publicly disclosed and may be utilized. The vendor explains: "We don't consider this an independently exploitable vulnerability. The only path to controlling `use_function`/'configuration_value` in the `configuration` table is the SQL Patch tool (raw arbitrary SQL execution) or a pre-existing SQL injection elsewhere".	4.1	More Details
	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the edit_user capability could create a native Splunk username that ends with a period. The vulnerability is possible because username validation does not reject a trailing period before the username is used for a user directory. This can cause distinct native Splunk usernames to share per-user configuration data, and user-		

CVE-2026-76277	management operations can affect the wrong account or fail. For more information see Set up native Splunk authentication (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/use-the-native-splunk-platform-authentication-scheme/set-up-native-splunk-authentication) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	4.1	More Details
CVE-2026-97354	The PowerPress Podcasting plugin by Blubrry WordPress plugin before 11.17.11 does not validate the destination of redirects when fetching a user-supplied media URL, allowing users with the contributor role and above to perform Server-Side Request Forgery attacks against internal services.	4.1	More Details
CVE-2026-84224	The Kirki WordPress plugin before 6.3.2 does not validate the host of a URL it is given before fetching it, allowing users with editor-level access and above to make the site issue requests to internal services that are not otherwise reachable, and to tell which of those are live from the response.	4.1	More Details
CVE-2026-93694	In Progress ShareFile Storage Zones Controller v5.12.6 and below, processing of queue items can send acknowledgements to an unvalidated callback URL, this behavior together with a race condition allows the attacker to cause FileCopyService to consume attacker-controlled metadata and content. Exploitation requires control over copy queue work and a race condition.	4.0	More Details
CVE-2026-101886	Cisco Jabber for Android (com.cisco.im) before 15.3.1.311364 contains a path traversal vulnerability that allows a malicious app with no permissions to write attacker-controlled files into Jabber's private data directory by exploiting the exported crosslaunch.share activity and an unsanitized display name from a ContentProvider used in file path construction. Attackers can craft a shared content:// URI with a display name containing '..../' sequences to place fully attacker-controlled content within directories such as databases/, shared_prefs/, no_backup/, and files/ without user interaction.	4.0	More Details
CVE-2026-106438	An incorrect calculation in Decimal128 string parsing in the MongoDB C Driver can accept certain over-precision inputs containing leading zeros instead of rejecting them. This produces a value different from the supplied text. An actor who can provide a decimal string to an embedding application, including through Extended JSON parsing, can cause the application to store or use an incorrect numeric value.	4.0	More Details
CVE-2026-107835	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. Prior to 3.8.1, internal/cookies.ParseCookies in internal/cookies/cookies.go handles boundary ASCII control characters and control-only or empty cookie names differently from several backend cookie parsers. An unauthenticated attacker can craft a Cookie header so Coraza indexes or drops a cookie under a different name or value from the backend application, causing rules targeting REQUEST_COOKIES or REQUEST_COOKIES_NAMES to miss application-visible attacker data. Exploitation depends on the backend parser and affected rule scope, and interior control characters with inconsistent backend behavior are outside this advisory's remediation. This issue is fixed in version 3.8.1.	4.0	More Details
CVE-2026-107655	A flaw was found in CUPS. When processing embedded job ticket comments within documents, the service improperly handles specific IPP attributes, causing an unhandled null pointer dereference. An unauthenticated attacker permitted to submit jobs to a shared printer queue can send a crafted Internet Printing Protocol (IPP) request to crash the print daemon, resulting in a temporary Denial of Service (DoS) for all printing services.	4.0	More Details
CVE-2026-106580	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-31 and 6.9.13-56, a missing security-policy check in the CUT encoder allows a crafted local encoding operation to read data that policy should deny and can also cause a crash. This issue is fixed in versions 7.1.2-31 and 6.9.13-56.	4.0	More Details
CVE-2026-106566	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-32, delegate symlink cleanup does not check the MAGICK_SHRED_PASSES environment variable, allowing a local privileged workflow to overwrite a file with random data. This issue is fixed in version 7.1.2-32.	4.0	More Details
CVE-2026-107229	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. From 2.16.0 until 3.0.14, ThreadSafeCookieStore incompletely validates cookie Domain attributes. Missing private-section and default public-suffix rules, absent A-label normalization, locale-sensitive lowercasing, public-suffix host-only handling, and numeric or IP host checks allow one origin to store a cookie later sent to another origin. Applications sharing one client across trust domains can therefore receive attacker-injected cookies and may be exposed to session fixation. This issue is fixed in version 3.0.14.	4.0	More Details
CVE-2026-107825	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. From 3.0.0 until 3.8.0, ProcessURI in internal/corazawaf/transaction.go handles a url.ParseRequestURI failure by retaining the raw URI but leaving QUERY_STRING, ARGS_GET, ARGS_GET_NAMES, and the GET-derived portion of ARGS empty. An unauthenticated attacker can place control bytes in a URI passed directly by integrations such as coraza-spoa, coraza-proxy-wasm, custom FFI hosts, or WASM hosts, causing Coraza to omit query parameters that the downstream integration may still process and allowing rules targeting those variables to be	4.0	More Details

	bypassed. The bundled coraza/v3/http integration is not affected because Go net/http rejects such malformed request targets before calling Coraza. This issue is fixed in version 3.8.0.		
CVE-2026-87726	Insufficient API bounds checking in phalFelica in NXP NXPNfcRdLib RC663 through 07.14.00_Pub may allow an attacker with privileges or an untrusted third party to access unintended memory regions, potentially leading to limited loss of confidentiality, integrity, and availability. All software versions from 07.18.00 onwards have fixed this problem.	3.9	More Details
CVE-2026-78017	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Check for Unusual or Exceptional Conditions vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering and Protection mechanism bypass.	3.8	More Details
CVE-2026-107269	Gophish through 0.12.1 contains a timing discrepancy vulnerability in AdminServer.Login that allows unauthenticated attackers to enumerate valid usernames by measuring login response times. Attackers can submit candidate usernames to POST /login and detect bcrypt comparison delays for existing accounts, narrowing targets for password guessing or credential stuffing.	3.7	More Details
CVE-2026-107727	Strawberry GraphQL is a library for creating GraphQL APIs. From 0.312.3 until 0.327.2, the legacy graphql-ws subscription handler in strawberry/subscriptions/protocols/graphql_ws/handlers.py does not remove naturally completed operations from self.tasks and self.subscriptions. When max_subscriptions_per_connection is configured, a client on a persistent WebSocket connection can use distinct operation IDs for one-shot subscriptions to fill the connection's configured slots even after those subscriptions send complete, causing later legitimate operations on that connection to be rejected with Subscription limit reached. The modern graphql-transport-ws protocol and deployments without the configured per-connection cap are not affected. This issue is fixed in version 0.327.2.	3.7	More Details
CVE-2026-106428	An out-of-bounds read in SCRAM authentication response parsing in the MongoDB C Driver can read one byte beyond a fixed-size buffer when processing a malformed server-final message. A server or network intermediary able to provide this message before server-signature verification can cause the application using the driver to terminate. The extra byte is not returned through the protocol.	3.7	More Details
CVE-2026-108749	docling-serve 1.14.0 through 1.36.0 contains a missing authentication vulnerability that allows unauthenticated attackers to access /v1/memory/stats and /v1/memory/counts because they omit the require_auth dependency. Attackers can bypass the configured DOCLING_SERVE_API_KEY to read process and cgroup memory telemetry, object type histograms, and force repeated gc.collect() heap enumeration.	3.7	More Details
CVE-2026-107296	msgpack5 is a msgpack v5 implementation for node.js and the browser. Prior to 6.1.0, decoding a negative signed 64-bit integer modifies the corresponding bytes in the caller-provided input buffer while computing the value. Applications that retain or reuse encoded input for integrity checks, logging, or later processing can observe silently corrupted data, while positive integers and other MessagePack value types are unaffected. This issue is fixed in version 6.1.0.	3.7	More Details
CVE-2026-104006	The SpeedyCache - Cache, Optimization, Performance plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2 via the 'comment_author_*, comment_author_email_*' parameter. This makes it possible for unauthenticated attackers to extract the full name and email address of returning commenters pre-filled into comment form input fields and persisted as the site-wide cached page by any unauthenticated attacker requesting the same public URL. The read-side handler in advanced-cache.php correctly skips cached delivery for requests carrying comment_author_* cookies, but this check is absent on the write path, meaning the cache poisoning is invisible to the victim commenter yet fully exploitable by any unauthenticated attacker with no cookies.	3.7	More Details
CVE-2026-108736	Speedtest Tracker through 1.15.0 contains an IP allowlist bypass vulnerability that allows unauthenticated remote attackers to evade ALLOWED_IPS and Prometheus allowlists by spoofing X-Forwarded-For headers. Because bootstrap/app.php trusts every peer as a proxy, attackers can supply an allowlisted address to read /prometheus metrics and reach protected web and API endpoints.	3.7	More Details
CVE-2026-78021	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Generation of Error Message Containing Sensitive Information vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and Information exposure.	3.7	More Details
CVE-2026-107284	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.12 and 2.16.1, WebSocketHandler.upgrade aborts a handshake whose Sec-WebSocket-Accept value is missing or invalid but continues into pipeline installation and onOpen delivery. Frames coalesced with the invalid 101 response can be decoded and delivered from a peer that did not prove the handshake, although the request future fails and the channel closes. This issue is fixed in versions 3.0.12 and 2.16.1.	3.7	More Details
CVE-2026-107283	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.12 and 2.16.1, Realm.Builder generates the HTTP Digest client nonce with ThreadLocalRandom rather than a cryptographically secure random source. Digest relies on an unpredictable nonce to resist chosen-plaintext and credential precomputation attacks, so an observer able to infer generator state can reduce the protection of the authentication exchange. This issue is fixed in	3.7	More Details

	versions 3.0.12 and 2.16.1.		
CVE-2026-12091	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 could allow a denial of service due to a heap-based out-of-bounds read. A remote attacker could send a specially crafted request that causes a limited out-of-bounds memory read.	3.7	More Details
CVE-2026-78015	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Use of Less Trusted Source vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information tampering.	3.7	More Details
CVE-2026-107288	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.77.0 until 1.107.6 and 2.44.0, the local web_fetch_tool and the WebFetch local fallback compare blocked_domains entries with a URL hostname before both values are normalized to the form used by getaddrinfo. An attacker-influenced model can use an equivalent IDNA spelling, non-ASCII label separator, case variation, or trailing root label that resolves to a blocked host but does not match the configured string, causing the application to fetch that host with its own privileges. allowed_domains fails closed for unmatched spellings, and private-IP and cloud-metadata protections remain effective. This issue is fixed in versions 1.107.6 and 2.44.0.	3.7	More Details
CVE-2026-96393	The Affinity by Canva app before 3.3.1 (October 2026 release) did not perform adequate bounds checking when parsing Affinity document files, leading to an out-of-bounds pointer dereference. A threat actor could craft an Affinity document that, when opened by a user in Affinity, could result in an application crash.	3.6	More Details
CVE-2026-108981	ngx_cache_purge before 3.0.4 can allow file deletion via a symlink attack in certain situations where nginx and a served application (e.g., WordPress) run under the same user account. The attacker must be able to create a symlink inside the cache path. Version 3.0.4 fixes this for the case of a symlink created at an arbitrary earlier time, but does not resolve an applicable TOCTOU race condition. (The ngx_cache_purge module follows symlinks while walking the cache directory tree during purge operations. The module relies on nginx's ngx_walk_tree(), which relies on stat() and therefore follows symlinks.)	3.6	More Details
CVE-2026-101094	The Affinity by Canva application before 3.3.1 (October 2026 release) did not correctly handle incomplete UTF-8 character sequences when parsing text in Affinity document files, leading to a heap buffer over-read. A threat actor could craft an Affinity document that, when opened by a user in Affinity, could disclose the contents of adjacent heap memory in the document's text or result in an application crash.	3.6	More Details
CVE-2026-101130	The Affinity by Canva application before 3.3.1 (October 2026 release) did not perform adequate bounds checking when parsing arrays of strings in Affinity document files, leading to a heap buffer over-read. A threat actor could craft an Affinity document that, when opened by a user in Affinity, could disclose the contents of adjacent heap memory in the document's text or result in an application crash.	3.6	More Details
CVE-2026-106432	The BSON encoder in the MongoDB PHP Driver converts a string length to a 32-bit value without validation. When an affected application encodes a string near 4 GiB, the allocation size can wrap while the copy operation uses the original length. The resulting heap buffer overflow can corrupt process memory or terminate the PHP process. Reaching this issue requires a non-default runtime configuration that permits multi-gigabyte values. No MongoDB server interaction is required.	3.6	More Details
CVE-2026-105081	ImageMagick before 6.9.13-58 and 7.x before 7.1.2-33 does not properly account for symbolic links in the IsRightsAuthorizedByName security policy check, allowing configured policy restrictions to be bypassed. Local attackers who can create a symlink can point it at a policy-restricted path to evade the configured policy.	3.6	More Details
CVE-2026-96395	The Affinity by Canva app for macOS before 3.3.1 (October 2026 release) did not perform adequate bounds checking when generating QuickLook thumbnails and previews of Affinity document files, leading to an out-of-bounds heap read. A threat actor could craft an Affinity document that, when displayed or previewed by a user in Finder, could disclose the contents of adjacent heap memory, including memory addresses, in the rendered thumbnail or preview image.	3.6	More Details
CVE-2026-104754	The Rank Math SEO WordPress plugin before 1.0.280 does not escape a stored redirection source value before outputting it in an administrative list view, allowing users who can manage redirections (Administrators by default) to store JavaScript that executes in the session of any user who later opens that view, including a Super Administrator on multisite.	3.5	More Details
CVE-2026-89290	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in İzometri IT Services Domestic and Foreign Trade Co. Ltd. Eimzamip allows Stored XSS. This issue affects eimzamip: from v1.6.4 before v1.6.7.	3.5	More Details
CVE-2026-108809	A vulnerability was identified in Eleveo Call Recording Software up to 10.3.0. This issue affects some unknown processing of the file /auth/realms/default/protocol/openid-connect/logout. The manipulation leads to session expiration. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-	Contao is an Open Source CMS. From version 4.0.0 until 5.3.50 and 5.7.12, RequestTokenListener validates REQUEST_TOKEN only for POST requests, while the declarative GET guard runs only when an act parameter is present. Backend actions dispatched through the key parameter can therefore execute without a CSRF token		More

2026-107848	when an authenticated backend user loads an attacker-controlled URL. Reachable actions remain limited to modules available to that user, and the advisory demonstrates destructive or state-changing actions rather than privilege escalation. This issue is fixed in versions 5.3.50 and 5.7.12.	3.5	Details
CVE-2026-108566	A vulnerability has been found in InstantSoft icms2 up to 2.18.2. This issue affects the function index of the file templates/default/controllers/messages/index.tpl.php of the component Private Message Handler. Such manipulation of the argument nickname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 3a1ec8fcb073a46d06a2ab83bc2bf68225834281. It is best practice to apply a patch to resolve this issue.	3.5	More Details
CVE-2026-108815	A vulnerability has been found in idcCMS 1.70. Affected is an unknown function of the file admin/member_deal.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-108802	A weakness has been identified in y_project RuoYi up to 4.8.3. This affects the function renderDrawer of the file /system/dict/data/add of the component Dictionary Data Drawer Preview. Executing a manipulation of the argument cssClass can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-15703	The HireZoot WordPress plugin before 4.0.0 does not sanitise and escape one of its job specification settings before it is reflected back into an admin-area settings page, allowing users with the HireZoot WordPress plugin before 4.0.0's management capability (Administrator by default) to store a payload that is executed in the browser of any administrator who later opens that page. As the unfiltered_html capability is not available to administrators on multisite (or where DISALLOW_UNFILTERED_HTML is set), this leads to Stored Cross-Site Scripting.	3.5	More Details
CVE-2026-108594	Mealie 3.26.0 through 3.28.0 contains a server-side request forgery vulnerability in the OpenID Connect avatar fetch that ignores ports when allowlisting the identity provider hostname. Authenticated OIDC users who control their picture URL can make the server send GET requests to arbitrary ports on the provider's internal address on each login.	3.5	More Details
CVE-2026-107448	Magic: The Gathering Arena (Windows/Steam client; 2026.59.30.12801.127931.6 and certain later 2026.60.x builds) passes a server-supplied URL from a home-screen carousel GoToExternalUrl action directly to the Windows shell via Application.OpenURL/ShellExecuteW without validating the URI scheme or domain. A hypothetical attacker able to control the carousel content delivered to clients can cause arbitrary registered URI-scheme handlers to be invoked on client hosts with no user interaction. For example, one might expect that the carousel content only has https: URIs, not ms-calculator: URIs.	3.4	More Details
CVE-2026-107449	linuxserver Heimdall through 2.8.3 applies its SafeUrlFetcher SSRF protection mechanism only to ItemController; the enhanced-application test and live-stats requests occur via SupportedApps::execute(), a GuzzleHttp client that lacks IP address restrictions. In some realistic installations, the POST /test_config (and GET /get_stats) endpoints are accessible through CSRF, and thus an unauthenticated attacker can force the server to send requests to arbitrary internal hosts and ports (including 169.254.169.254) and read a status/port oracle in addition to partial response data.	3.4	More Details
CVE-2026-18418	The zbus proxy agent IPC backend in subsys/zbus/proxy_agent/zbus_proxy_agent_ipc.c logged the channel name of a rejected inter-domain frame with a plain %s conversion. The frame type struct zbus_proxy_msg carries a fixed-size channel_name[] array as its last member, and nothing in the transport guarantees the array is NUL-terminated. The only code that verifies termination is zbus_proxy_agent_receive_cb() in subsys/zbus/proxy_agent/zbus_proxy_agent.c, which rejects the frame in precisely those cases — so the warning printed a non-terminated buffer exactly on the error paths where the name had been found invalid (or, for an invalid message_size, had not been inspected at all). Any peer domain able to place a frame of sizeof(struct zbus_proxy_msg) bytes on the bound ipc_service endpoint can trigger it, by sending a frame with an out-of-range message_size or with channel_name[] containing no NUL byte. Reaching the code requires CONFIG_ZBUS_PROXY_AGENT_IPC and logging built at warning level or above (the default), and requires control over the firmware of the peer domain — typically a second core on the same SoC. The resulting strlen() inside the log packager walks past the end of the frame object until it finds a zero byte. With the icmsg backend the frame lives in a stack buffer of the IPC work-queue thread, so bytes of that thread's stack are rendered into the log message; with the rpmsg backends the scan continues through the shared vring memory. Impact is bounded to disclosure of a small amount of adjacent memory into the receiving domain's log sink, plus a possible fatal fault if the scan leaves a mapped region; the log packager's own -ENOSPC bound prevents the overrun from becoming a write. The fix bounds the conversion with %.*s and MIN(msg->channel_name_len, sizeof(msg->channel_name)).	3.4	More Details
CVE-2026-107890	OpenPrinting CUPS before 2.4.20 contains a NULL pointer dereference caused by repeated IPP group tags in job-creation requests. IPP parsing creates unnamed separator attributes with IPP_TAG_ZERO, but add_job() converts these separators to IPP_TAG_JOB. During job startup, get_options()/ipp_length() subsequently calls strlen() on a NULL attribute name, terminating cupsd and disrupting all queues. A single crafted Print-Job request can trigger the crash when the client can reach the scheduler and submit jobs to an accepting, enabled queue supporting the submitted document format. Anonymous submission is possible when	3.3	More Details

	permitted by listener and access-control configuration.		
CVE-2026-108851	phpMyFAQ through 4.1.10 contains a missing authorization vulnerability in the MCP server faq_search tool that allows MCP clients to read restricted FAQs because Search::searchDatabase() never applies user or group permission checks. Attackers connected to the phpmyfaq:mcp:server can issue search queries to retrieve the full question and answer text of active FAQs restricted to specific users or groups.	3.3	More Details
CVE-2026-108603	slide-maker through 5.8.0 contains a path traversal vulnerability in generate_images_openai.py that allows attackers to write image files outside the output directory via manifest-supplied filenames. Attackers can influence deck source material so the image prompt manifest contains ../ or symlinked filenames, creating directories and overwriting existing files at arbitrary paths.	3.3	More Details
CVE-2026-108857	Hugging Face Text Embeddings Inference through 1.9.4 contains a cleartext logging vulnerability that exposes the configured api_key because the router's Args struct lacks a redact attribute for it. Attackers with access to router logs, container output, or OTLP telemetry can recover the Bearer token and call the protected embedding and rerank endpoints.	3.3	More Details
CVE-2026-108502	ZTE Z80 Ultra contains an information disclosure vulnerability, through which third-party applications can read relevant information by hooking system APIs.	3.3	More Details
CVE-2026-108503	ZTE Z80 Ultra has an interface permission validation vulnerability. The callable functions provided by the system lack sufficient access control. An attacker can leverage these functions to read relevant information.	3.3	More Details
CVE-2026-108505	ZTE Z80 Ultra has a local information disclosure vulnerability. Third-party applications can capture data returned by system interfaces to obtain device-related information.	3.3	More Details
CVE-2026-106095	The Code Snippets WordPress plugin before 3.10.0 does not perform a capability check on one of its snippet-management actions and derives the network scope of the targeted snippet from the request instead of from the stored record, allowing an administrator of a single subsite on a multisite network to activate, deactivate and reprioritise network-scoped snippets that run across every site in the network.	3.3	More Details
CVE-2026-107676	FFmpeg through 9.0.2 contains an uninitialized memory disclosure vulnerability in av_dynamic_hdr_plus_to_t35() that leaves up to three payload bytes uninitialized when tone_mapping_flag is 0. Attackers can supply crafted Matroska T.35 BlockAdditional or HEVC/AV1 SEI metadata so that remuxing or transcoding writes leaked process memory into output files.	3.3	More Details
CVE-2026-105196	The Appointment Booking Plugin WordPress plugin before 5.6.9 does not enforce per-record authorization on several of its AI Abilities API actions, allowing an authenticated user holding the LatePoint Agent role, normally restricted to their own records, to read and modify other agents' profile data and read other agents' bookings and associated customer details when the Abilities API feature is enabled.	3.3	More Details
CVE-2026-107885	OpenPrinting CUPS through 2.4.20 contains a resource-exhaustion vulnerability in the submission-timeout handling of cupsdCheckJobs(). The scheduler suppresses timeout processing for all pending jobs whenever any client connection has an in-flight Send-Document operation, without matching that connection to the job being examined. A client allowed to reach the IPP service can hold an incomplete HTTP request containing parsed Send-Document headers before operation authorization, preventing unrelated incomplete jobs from expiring. Where Create-Job submission is allowed, incomplete jobs can accumulate until MaxJobs is exhausted and further legitimate print submissions are rejected. The suppression ends when the held connection closes.	3.3	More Details
CVE-2026-108754	GPT-Load through 1.4.11 contains a cleartext logging vulnerability that exposes client proxy keys because the Gin Logger middleware records the raw query string before extractAuthKey strips the key parameter. Attackers with read access to console logs or ./data/logs/app.log can recover proxy keys from Gemini-style requests and use them against the corresponding group.	3.3	More Details
CVE-2026-87980	IBM Guardium Data Protection 12.0, 12.1, and 12.2 could allow a local attacker to obtain sensitive information due to cleartext storage of sensitive information in logs.	3.1	More Details
CVE-2026-108745	CloudBeaver through 25.3.5 contains a missing authorization vulnerability in WebSQLResultServlet that allows any web session holder to read other users' LOB export files from a shared folder. Attackers can guess table and column names and enumerate second-resolution timestamps to download victims' LOB values, including data from connections they cannot query.	3.1	More Details
CVE-2026-78016	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Validation of Specified Type of Input vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure and Information tampering.	3.1	More Details
CVE-	The AI Puffer – Chat. Create. Automate. (formerly AI Power) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.4.89. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers,		

2026-104742	with subscriber-level access and above, to modify global site-wide semantic search settings, including vector provider, embedding provider, embedding model, target ID, number of results, and no-results text stored in aipkit_options, that are otherwise restricted to administrators. Exploitation requires that an administrator has previously granted the Knowledge Base ('sources') module to the attacker's role via the Role Manager, as this access is not available to lower-privileged users by default.	3.1	More Details
CVE-2026-104741	The AI Puffer – Chat. Create. Automate. (formerly AI Power) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.4.89. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify global plugin indexing and vector-search configuration options (aipkit_training_general_settings and aipkit_indexing_field_settings), including chunking parameters, file upload visibility, and per-CPT field indexing settings, affecting all users of the plugin. This is only exploitable in configurations where an administrator has granted 'sources' module access to a lower-privileged role via the plugin's Role Manager.	3.1	More Details
CVE-2026-108741	Shepherd (shepherd-ai) through 0.3.1 contains a server-side request forgery guard bypass in the citation-checker extra because the public_url guard validates a resolved address but fetch re-resolves the hostname at connect time. Attackers who plant a crafted reference URL in a checked document and control its DNS can rebind it to internal addresses, sending GET requests to internal HTTP(S) services and capturing responses in evidence files.	3.1	More Details
CVE-2026-87108	An authenticated Ops Manager user with a read-only project role can retrieve a daily host monitoring record associated with a different project when they possess the required record identifier. Insufficient ownership validation can expose deployment metadata, including host and configuration details.	3.1	More Details
CVE-2026-107170	A flaw was found in m17n-lib. A partial failure during library initialization can leave an internal driver pointer uninitialized. Under specific error conditions, such as system resource exhaustion or database corruption, an application attempting to open an input method dereferences this null pointer without proper validation. This issue causes the application to crash, resulting in a Denial of Service (DoS).	2.9	More Details
CVE-2026-96394	The Affinity by Canva application for macOS before 3.3.1 (October 2026 release) did not validate image dimensions against the size of the pixel data when generating QuickLook thumbnails and previews of Affinity document files, leading to an out-of-bounds heap read. A threat actor could craft an Affinity document that, when displayed or previewed by a user in Finder, could disclose the contents of adjacent heap memory in the rendered thumbnail or preview image, or cause the thumbnail or preview extension to crash.	2.9	More Details
CVE-2026-11939	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 may be vulnerable to audit log forgery.	2.7	More Details
CVE-2026-105197	The Appointment Booking Plugin WordPress plugin before 5.6.5 does not verify that a backend staff user is authorized to act on the specific record targeted for deletion, allowing an authenticated user with a record-scoped staff role to irreversibly delete any order, customer, or transaction on the site, including records belonging to other staff and outside their assigned scope.	2.7	More Details
CVE-2026-107694	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.2.0 does not verify that the vendor a commission calculation is requested for is the requesting vendor, allowing vendors to disclose the commission rate and fixed fee the marketplace administrator configured for other vendors.	2.7	More Details
CVE-2026-107507	The Squadeno WordPress plugin before 1.12.0 does not enforce its restrictions on every way a sport can be saved, allowing users with the lowest-tier Trainer role to change the section, age group, author, password, comment settings and date of a sport they are assigned to.	2.7	More Details
CVE-2026-104684	The Envira Gallery WordPress plugin before 1.16.2 does not verify that a user is authorized to read a gallery before rendering it, allowing authors to embed and expose other users' non-public gallery metadata to unauthenticated visitors.	2.7	More Details
CVE-2026-104682	The Envira Gallery WordPress plugin before 1.16.2 does not correctly check authorization on its gallery-conversion feature, verifying that the requester can edit an arbitrary post they name rather than that they are allowed to create the Envira Gallery WordPress plugin before 1.16.2's own gallery content, allowing users with contributor-level access to create and publish gallery posts that the Envira Gallery WordPress plugin before 1.16.2's settings otherwise withhold from them.	2.7	More Details
CVE-2026-105195	The Booking Calendar WordPress plugin before 11.8.3 does not adequately restrict which options a lower-privileged user can load through one of its settings handlers, allowing users with the Editor role and above to disclose the values of arbitrary WordPress options, including core site configuration.	2.7	More Details
CVE-2026-104645	The Image Photo Gallery Final Tiles Grid WordPress plugin before 3.6.14 does not properly verify authorization on several of its gallery and image management actions, checking ownership against a different object than the one being acted on, or omitting the check entirely, allowing any authenticated user with contributor-level access or above to clone, modify and reorder galleries and images belonging to other	2.7	More Details

	users and to write Image Photo Gallery Final Tiles Grid WordPress plugin before 3.6.14 metadata onto arbitrary posts they do not own.		
CVE-2026-94258	The SMS Alert WordPress plugin before 4.0.1 does not check that the acting administrator is allowed to manage the selected users before returning their stored billing phone numbers, allowing an administrator of one site on a multisite network to disclose the phone numbers of users who belong to other sites on that network. This affects multisite only, and requires the SMS Alert WordPress plugin before 4.0.1's gateway credentials to be stored on the acting administrator's own site.	2.7	More Details
CVE-2026-104678	The CP Media Player WordPress plugin before 1.3.4 does not perform a capability check on its settings-page handler, allowing users with only Contributor-level access to create, modify, duplicate and delete the site-wide media player configurations and change a CP Media Player WordPress plugin before 1.3.4 option that should require administrator access.	2.7	More Details
CVE-2026-104681	The Envira Gallery WordPress plugin before 1.16.2 does not verify that an image identifier added to a gallery refers to a media attachment the caller is permitted to view, allowing any user able to create and edit a gallery (Author and above by default) to disclose the title and excerpt of other users' private, draft, pending and trashed posts that WordPress would otherwise withhold from them.	2.7	More Details
CVE-2026-108808	A vulnerability was determined in Eleveo Call Recording Software up to 10.3.0. This vulnerability affects unknown code of the file /auth/realms/default/protocol/openid-connect/logout of the component JWT Token Handler. Executing a manipulation of the argument id_token_hint can lead to use of get request method with sensitive query strings. The attack may be launched remotely. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. 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.	2.6	More Details
CVE-2026-106583	In ssh in OpenSSH before 10.6, a \$ or \ character can occur in a command-line username, leading to injection.	2.5	More Details
CVE-2026-108723	answer-me-with-html through 0.5.0 contains a link following vulnerability in the am CLI code block src= embedding, where localPath() checks only path text without resolving symlinks. Attackers can ship a repository with a symlink pointing outside the checkout so am render embeds readable external files into generated HTML, disclosing them when shared.	2.5	More Details
CVE-2026-107570	heap OOB write in convert_file_from_to() via a crafted Content-Type header allows attacker to OOB write when email is used as a template.	2.5	More Details
CVE-2026-107886	OpenPrinting CUPS before 2.4.20 contains a double-free in printer-class management. When CUPS-Add-Modify-Class replaces an existing class member list, add_class() frees pclass->printers without clearing the pointer. If subsequent validation fails, the class retains the dangling pointer; CUPS-Delete-Class subsequently frees the same allocation in cupsdDeletePrinter(). A client authorized to modify and delete classes can cause scheduler-wide denial of service. The default policy requires @SYSTEM privileges.	2.3	More Details
CVE-2026-105977	The Portfolio Filter Gallery WordPress plugin before 2.2.1 does not perform a per-object authorization check before deleting an attachment, allowing users with the Contributor role and above to permanently delete certain media attachments belonging to other users, including administrators.	2.2	More Details
CVE-2026-21135	Improper access control in Samsung Internet prior to version 30.0.5.6 allows local attackers to access sensitive information.	N/A	More Details
CVE-2026-21137	Path traversal in Smart Switch prior to version 3.7.73 allows physical attackers to access files with Smart Switch privilege.	N/A	More Details
CVE-2026-107104	This vulnerability exists in the ERP system due to unsafe deserialization of user controlled data in the affected functionality. An unauthenticated remote attacker could exploit this vulnerability by supplying specially crafted data to the vulnerable functionality of the targeted system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code, manipulate application data or perform other unintended actions on the targeted system.	N/A	More Details
CVE-2026-21129	Improper input validation in GuestCreditCardRegisterActivity of Samsung Checkout prior to version 5.1.03.1 allows local attackers to launch an arbitrary activity with Samsung Checkout privileges.	N/A	More Details
CVE-2026-107726	Hazelcast is a unified real-time data platform combining stream processing with a fast data store. Prior to 5.4.5, 5.5.10, and 5.6.1, improper validation of data supplied by a malicious client able to connect to a cluster allows arbitrary reads from a cluster member's Java heap, off-heap data, and JVM process address space. The same flaw can crash cluster members and, in some Hazelcast Enterprise Edition configurations, corrupt memory with possible arbitrary code execution. Both slim and full distributions are affected. This issue is	N/A	More Details

	fixed in versions 5.4.5, 5.5.10, 5.6.1, and 5.7.0.		
CVE-2026-58068	This vulnerability in Veeam Agent for Microsoft Windows allows any local user to terminate arbitrary processes on the system.	N/A	More Details
CVE-2026-21131	Incorrect default permission in Samsung Flow prior to version 4.9.22.4 allows local attackers to launch an arbitrary activity with Samsung Flow privileges on the connected device.	N/A	More Details
CVE-2026-21130	Improper input validation in CreditCardRetrieveActivity of Samsung Checkout prior to version 5.1.03.1 allows local attackers to launch an arbitrary activity with Samsung Checkout privileges.	N/A	More Details
CVE-2026-21132	Improper input validation in Samsung Internet prior to version 30.0.5.24 allows remote attackers to inject arbitrary script. User interaction is required for triggering this vulnerability.	N/A	More Details
CVE-2026-21133	Path traversal in Samsung Flow prior to version 4.9.22.1 allows local attackers to access clipboard data.	N/A	More Details
CVE-2026-21134	Improper authentication in Samsung Flow prior to version 4.9.22.4 allows adjacent attackers to access sensitive information.	N/A	More Details
CVE-2026-21138	Insufficient verification of data authenticity in Smart Switch prior to version 3.7.73 allows physical attackers to install arbitrary applications.	N/A	More Details
CVE-2026-21139	Improper access control in Samsung Continuity Service for windows prior to version 4.6.1217.0 allows adjacent attackers to manipulate the connected mobile device.	N/A	More Details
CVE-2026-21136	Improper authorization in Smart Switch prior to version 3.7.73 allows physical attackers to invoke application restore process.	N/A	More Details
CVE-2026-107736	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, MaybeFlipBitmap() asks GDI+ to read the attacker-controlled PropertyTagOrientation size through GetPropertyItem() while supplying only a fixed 64-byte buf on the stack. Opening a crafted TIFF with enough EXIF Orientation values can cause attacker-selected bytes to overwrite stack control data, while tested builds terminate through the stack cookie check. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
CVE-2026-92543	Docker Engine classifies a registry hostname as insecure using an any-match DNS check. loadInsecureRegistries() injects 127.0.0.0/8 and ::1/128 as insecure CIDRs by default. isCIDRMatch resolves all of the hostname's addresses and returns true if a single address is in the insecure CIDR list. Because the transport re-dials the hostname rather than the CIDR-matching address, a DNS answer set of one loopback IP plus a non-loopback attacker IP disables certificate verification and enables HTTP fallback for the registry connection.	N/A	More Details
CVE-2026-21128	Improper input validation in CreditCardRegisterActivity of Samsung Checkout prior to version 5.1.03.1 allows local attackers to launch arbitrary activity with Samsung Checkout privileges.	N/A	More Details
CVE-2026-62163	Rejected reason: Reason: This candidate is a duplicate of CVE-2026-60089.	N/A	More Details
CVE-2026-107725	Hazelcast is a unified real-time data platform combining stream processing with a fast data store. Prior to 5.4.5, 5.5.10, and 5.6.1, missing authorization checks in the IMap Predicates API allow a malicious client with limited privileges to execute arbitrary code on a Hazelcast cluster member. This issue is fixed in versions 5.4.5, 5.5.10, 5.6.1, and 5.7.0.	N/A	More Details
	Improper Certificate Validation vulnerability in hexpm hex_core allows an attacker who can intercept HTTPS connections to impersonate hex.pm, repo.hex.pm or any other repository or API server to programs that use hex_core's default HTTP adapter on Erlang/OTP 24, or on OTP 25 when the operating system's CA certificates can't be loaded. hex_core:default_config/0 selects the built-in hex_http_httpc adapter. For an HTTPS request whose adapter config has no ssl option, hex_http_httpc:http_options/2 builds options that verify the server certificate against public_key:cacerts_get/0. When that call raises, the adapter prints a warning and sends the request without ssl options, so httpc uses the defaults of the ssl application, which before OTP 26 don't verify the server certificate. public_key:cacerts_get/0 doesn't exist on OTP 24, so every HTTPS request falls back		

CVE-2026-103502	there, and on OTP 25 it raises when no CA store is found. hex_core versions before 0.11.0 never set ssl options, so they don't verify the server certificate on OTP 25 and earlier whether or not a CA store is found. The fallback was intended and documented, but the documentation didn't make clear that it meant no certificate verification. Since hex_core 0.8.2 the README has warned that the built-in httpc adapter "has insecure default settings" and recommended other HTTP clients, and the adapter prints "using default ssl options which are insecure" on every request that falls back. hex_core 0.11.0 added certificate verification with the changelog entry "Use secure SSL defaults for OTP 25+". Neither the README nor the warning says that the server certificate isn't verified, the README doesn't say which OTP versions the warning applies to, and on OTP 25 without CA certificates the warning tells users to upgrade to OTP 25 or later, which they already run. This advisory is published so that users who took those notices as general advice know their HTTPS requests weren't authenticated. This issue affects hex_core: from 0.1.0 before 0.20.0.	N/A	More Details
CVE-2026-62167	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-108982	VeraCrypt 1.26.29 (FUSE-T build) on macOS sometimes allows unintended access to decrypted data. It does not terminate the FUSE-T auxiliary service (go-nfsv4) and its associated VeraCrypt core-service helper processes when a volume is dismounted. After VeraCrypt reports the volume as dismounted, the auxiliary mount continues to serve the decrypted volume image (volume.dmg) over a loopback SMB session, and the leaked processes retain an open handle to the underlying raw device. A local user or process can therefore remount and access the decrypted volume without the passphrase, e.g., by reopening a previously accessed path (such as through a macOS Open Recent menu) or by attaching volume.dmg from the stale auxiliary mount. (The macOS FUSE build of VeraCrypt is not affected.)	N/A	More Details
CVE-2026-107716	Banks generates meaningful LLM prompts using a simple template language. Prior to 2.5.1, Banks DirectoryPromptRegistry does not reject symbolic links for index.json or discovered and existing .jinja prompt files. In an application where untrusted users can influence a prompt directory, DirectoryPromptRegistry._scan() and DirectoryPromptRegistry.get() can follow a link outside the registry root and disclose a file, while DirectoryPromptRegistry.set(), DirectoryPromptRegistry._save(), and DirectoryPromptRegistry._load() can read or overwrite an external link target. The issue requires attacker influence over the registry directory or its extracted contents. This issue is fixed in version 2.5.1.	N/A	More Details
CVE-2026-62166	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-107354	Rejected reason: ** This candidate has been removed by an organization.	N/A	More Details
CVE-2026-5703	Path traversal vulnerability in the Satel Iberia SenNet Datalogger Serie 200, specifically in the web portal provided by the device, which allows an authenticated user to read any file or list any directory accessible to the system user running the web server. This is possible by modifying the URL to include a path traversal payload. Successful exploitation of this vulnerability could allow an attacker to access critical system files containing confidential information.	N/A	More Details
CVE-2026-100227	Improper Verification of Cryptographic Signature vulnerability in Apache CXF's JAX-RS XML Security module. The JAX-RS XML Signature interceptors (XmlSigInHandler, XmlSigInInterceptor and the streaming XmlSecInInterceptor) did not ensure that the XML passed to the application was covered by the signature. An attacker with any document signed by a trusted key could wrap it in unsigned content, which the application would then treat as signed. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-93026	This vulnerability in Veeam Backup & Replication allows a Backup Viewer to modify the Enterprise Manager master key and stored antivirus update credentials.	N/A	More Details
CVE-2026-107937	In Apache CXF, the parser for multipart/MTOM attachment part headers did not fully enforce the configured attachment-max-header-size (default 300 characters) and attachment-headers-max-count (default 500) limits. The size limit was applied only to each physical line, not to a header value built from continuation lines or to the combined values of a repeated header. The count limit was checked against the number of distinct header names, not the total number of header lines. A remote, unauthenticated attacker could send a multipart request with very large folded or repeated part headers. The server would then allocate memory without bound, causing a denial of service. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-	In Apache CXF, the Netty-based HTTP client transport (cxf-rt-transport-http-netty-client) did not verify that the hostname in the server's TLS certificate matched the host being called. This applied over both HTTP/1.1 and HTTP/2, even when disableCNCheck was left at its default value of false. The certificate chain was validated against the configured trust store, but the endpoint's identity was not. A network attacker able to intercept traffic could present any certificate trusted by the client, such as a publicly issued certificate for a	N/A	More Details

107938	domain they control, and impersonate the target service. They could then read or modify the exchanged messages, including credentials. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.		
CVE-2026-108039	By default, StaxUtils placed no limit on the total number of elements or the total number of characters in an XML document. A very large request could therefore use a lot of memory and CPU during parsing, especially where CXF builds a DOM from the input (for example SAAJ or WS-Security), and could cause a denial of service when no request size limit was configured. Both limits now have defaults: the maximum element count is 100 × maxChildElements (5,000,000 by default), and the maximum document size is 256M characters. Applications that process larger documents can raise the limits with the org.apache.cxf.stax.maxElementCount and org.apache.cxf.stax.maxXMLCharacters properties. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-71575	The max_age authentication-freshness check in OidcClientCodeRequestFilter was inoperative due to a milliseconds/seconds unit mismatch and an inverted comparison polarity. Any relying party using setMaxAgeOffset to enforce re-authentication would silently accept sessions of any age, bypassing step-up authentication policies. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-107378	CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to 2.9.1, rendering an attacker-controlled SVG with a path containing many segments can cause quadratic CPU consumption in cairosvg/path.py. The path tokenizer repeatedly slices and rescans the remaining path data, while draw_markers drains node.vertices with node.vertices.pop(0), causing repeated linear-time work. The svg2png, svg2pdf, and svg2ps APIs reach these operations during ordinary rendering, allowing a sub-megabyte SVG to consume substantial CPU and deny service to a rendering application. This issue is fixed in version 2.9.1.	N/A	More Details
CVE-2026-58069	This vulnerability in Veeam Backup & Replication allows an authenticated Cloud Connect tenant to read arbitrary files on the service provider host.	N/A	More Details
CVE-2026-21127	Improper export of android application components in Samsung Account prior to version 15.7.01.1 allows local attackers to access sensitive data.	N/A	More Details
CVE-2026-21120	Use after free in WSM service prior to SMR Oct-2026 Release 1 allows local attackers to potentially execute arbitrary code with system privilege.	N/A	More Details
CVE-2026-21126	Improper input validation in getting cover image in libsimba.heifdec.media.samsung.so prior to SMR Oct-2026 Release 1 allows local attackers to write out-of-bounds memory.	N/A	More Details
CVE-2026-21125	Improper input validation in parsing sheifd in libsimba.heifdec.media.samsung.so prior to SMR Oct-2026 Release 1 allows local attackers to potentially execute arbitrary code.	N/A	More Details
CVE-2026-21124	Improper input validation in getting cover image in libsimba.heifdec.media.samsung.so prior to SMR Oct-2026 Release 1 allows local attackers to potentially execute arbitrary code.	N/A	More Details
CVE-2026-21123	Improper privilege management in Locksettings prior to SMR Oct-2026 Release 1 allows local privileged attackers with root privilege to access data of the tied profile in before first unlock.	N/A	More Details
CVE-2026-21122	Out-of-bounds write in libsamsungtts.so prior to SMR Oct-2026 Release 1 allows local attackers to execute arbitrary code.	N/A	More Details
CVE-2026-21121	Improper handling of insufficient permission in CmcCore prior to SMR Oct-2026 Release 1 allows local attackers to use the privileged APIs.	N/A	More Details
CVE-2026-21119	Out-of-bounds read and write in lib_sag_ai_sound_sep_v2.00.so prior to SMR Oct-2026 Release 1 allows local attackers to read and write out-of-bounds memory.	N/A	More Details
CVE-2026-62170	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-	Improper access control in DownloadProvider prior to SMR Oct-2026 Release 1 allows local attackers to	N/A	More

21118	access files in scoped storage.		Details
CVE-2026-21117	Improper access control in CocktailBarService prior to SMR Oct-2026 Release 1 allows local attackers to access sensitive information.	N/A	More Details
CVE-2026-21116	Out-of-bounds write in libsmkvextractor.so prior to SMR Oct-2026 Release 1 allows local attackers to write out-of-bounds memory.	N/A	More Details
CVE-2026-21115	Out-of-bounds write in libcodec2-sec-flacdec.so prior to SMR Oct-2026 Release 1 allows local attackers to write out-of-bounds memory.	N/A	More Details
CVE-2026-21114	Out-of-bounds write in libsmkvextractor.so prior to SMR Oct-2026 Release 1 allows local attackers to execute arbitrary code.	N/A	More Details
CVE-2026-92542	The firewall rules which mark VXLAN datagrams for encryption indiscriminately match both authentic VXLAN datagrams sent from the kernel and forged datagrams sent by user processes. Any packet sent from the host network namespace of a Linux Swarm node is encrypted with the overlay-network IPsec parameters which meets the following criteria: - UDP datagram - Destination port is the Swarm data-path port - Datagram starts with a VXLAN header for the VNI of an encrypted overlay network which any running container on the node is connected to	N/A	More Details
CVE-2026-102478	In affected versions of Octopus Server, an authenticated user with permission to modify roles could bypass the protections preventing access abuse resulting in privilege escalation. It was possible for the built-in role to be weakened and the attacker's account added to a privileged team. This was achievable due to improper validation of unsafe equivalence in inputs.	N/A	More Details
CVE-2025-64393	This vulnerability in Veeam Backup & Replication allows a Backup Viewer to execute arbitrary code as SYSTEM on the backup server.	N/A	More Details
CVE-2026-107103	This vulnerability exists in the ERP system due to insufficient validation and parameterization of user supplied input in an API endpoint. An unauthenticated remote attacker could exploit this vulnerability by supplying specially crafted input to the vulnerable endpoint. Successful exploitation of this vulnerability could allow the attacker to perform SQL injection attacks on the targeted system.	N/A	More Details
CVE-2026-105324	An HTTP header injection vulnerability in start-page-loader.cgi of ADM allows an unauthenticated remote attacker to read arbitrary files on the host system. By sending a crafted HTTP request with injected headers via the state parameter, the attacker can leverage the underlying web server's X-Sendfile mechanism to retrieve sensitive files without authentication. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RWC1 as well as from ADM 5.0.0 through ADM 5.1.4.RL21.	N/A	More Details
CVE-2026-104710	Rejected reason: Duplicate of CVE-2026-71364, which was publicly disclosed and fixed in Red Hat Ansible Automation Platform on 2026-08-24. No separate identifier is required.	N/A	More Details
CVE-2026-98381	In the Linux kernel, the following vulnerability has been resolved: veth: manage XDP program pointers during channel resize veth_set_channels() tears down XDP resources for removed RX queues without clearing rq->xdp_prog. If the program is then detached or replaced, those queues keep the old pointer after bpf_prog_put(). A later channel increase can re-enable NAPI and run the freed program. BUG: unable to handle page fault for address: fffff90000256048 Oops: Oops: 0000 [#1] SMP KASAN NOPTI RIP: veth_xdp_rcv_skb (include/linux/filter.h:779 include/net/xdp.h:696 drivers/net/veth.c:820) Call Trace: veth_xdp_rcv (drivers/net/veth.c:941) veth_poll (drivers/net/veth.c:986) __napi_poll (net/core/dev.c:7787) net_rx_action (net/core/dev.c:7850 net/core/dev.c:8007) handle_softirqs (kernel/softirq.c:645) Kernel panic - not syncing: Fatal exception in interrupt	N/A	More Details
CVE-2026-98380	In the Linux kernel, the following vulnerability has been resolved: net/sched: reject IDR error pointers when deleting actions tcf_action_delete() drops the reference held by its lookup before calling tcf_idr_delete_index() with the saved action index. An unlocked classifier can remove that action and reserve the same IDR slot with ERR_PTR(-EBUSY) in between. tcf_idr_delete_index() only checks the lookup result for NULL. It therefore treats the reservation as a tc_action and dereferences tca_bindcnt. A hardware execution breakpoint was used to schedule the interleaving without changing the kernel source. KASAN reported this decoded trace: BUG: KASAN: null-ptr-deref in tca_action_gd+0x5b9/0x1010 Read of size 4 at addr 0000000000000010 by task poc/150 Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002 RIP: tca_action_gd+0x5c0/0x1010: arch_atomic_read at arch/x86/include/asm/atomic.h:23 raw_atomic_read at include/linux/atomic/atomic-arch-fallback.h:457 atomic_read at include/linux/atomic/atomic-instrumented.h:33 tcf_idr_delete_index at net/sched/act_api.c:766 tcf_action_delete at net/sched/act_api.c:1859 tcf_del_notify at net/sched/act_api.c:2014 tca_action_gd at net/sched/act_api.c:2064 R13: 0000000000000010 R15: ffffffff00000000 Kernel panic - not syncing: Fatal exception R15 contains	N/A	More Details

	ERR_PTR(-EBUSY), and adding the tcfa_bindcnt offset produces the address in R13. With the guard applied, the same reproducer returned -ENOENT without a KASAN report or panic. Treat error pointers as absent and return -ENOENT.		
CVE-2026-98379	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_rpfilter: reject routes without inet6_dev ip6_route_lookup() can return an error-free route whose rt6i_idev is NULL. Lowering an external nexthop device's MTU below IPV6_MIN_MTU tears down its inet6_dev while fib6_ifdown() leaves routes using nexthop objects in the FIB. An unprivileged user can construct this state with rtnetlink in a private user and network namespace, then trigger a NULL dereference through an IPv6 rpfilter lookup: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000 KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: rpfilter_mt (net/ipv6/netfilter/ip6t_rpfilter.c:75) Call Trace: ip6t_do_table (net/ipv6/netfilter/ip6_tables.c:316) nf_hook_slow (net/netfilter/core.c:619) ipv6_rcv (net/ipv6/ip6_input.c:351) __netif_receive_skb_one_core (net/core/dev.c:6216) process_backlog (net/core/dev.c:6680) __napi_poll (net/core/dev.c:7739) net_rx_action (net/core/dev.c:7959) handle_softirqs (kernel/softirq.c:622) do_softirq.part.0 (kernel/softirq.c:523) __local_bh_enable_ip (kernel/softirq.c:450) __dev_queue_xmit (net/core/dev.c:4913) packet_sendmsg (net/packet/af_packet.c:3139) __sys_sendto (net/socket.c:2252) __x64_sys_sendto (net/socket.c:2259) do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) Kernel panic - not syncing: Fatal exception in interrupt Reject routes without an inet6_dev immediately after lookup. Such routes are not eligible for reverse-path filtering, and the check protects all later rt6i_idev dereferences.	N/A	More Details
CVE-2026-98378	In the Linux kernel, the following vulnerability has been resolved: bpf: Skip unsettled links in link iterator bpf_link_prime() inserts a link into link_idr before anon_inode_getfile() succeeds and before bpf_link_settle() publishes the ID in link->id. bpf_link_by_id() treats such an ID-zero link as unsettled, but the link iterator takes a reference without this check. If anon_inode_getfile() then fails, the creator removes the ID and frees its still-private link directly. The iterator is left with a dangling reference and its next bpf_link_put() accesses freed memory. Treat ID-zero entries as transient in bpf_link_get_curr_or_next(), just as bpf_link_by_id() does. BUG: KASAN: slab-use-after-free in bpf_link_put Write of size 8 by task exp/384 Call Trace: bpf_link_put kernel/bpf/syscall.c:3372 bpf_link_seq_next kernel/bpf/link_iter.c:33 bpf_seq_read kernel/bpf/bpf_iter.c:158 vfs_read fs/read_write.c:572 ksys_read fs/read_write.c:716 do_syscall_64 arch/x86/entry/syscall_64.c:84 entry_SYSCALL_64_after_hwframe arch/x86/entry/entry_64.S:121 Kernel panic - not syncing: KASAN: panic_on_warn set ...	N/A	More Details
CVE-2026-98377	In the Linux kernel, the following vulnerability has been resolved: vlan: require the MAC header to be present in __vlan_insert_inner_tag() __vlan_insert_inner_tag() only guarantees head room via skb_cow_head(), never that mac_len bytes of MAC header are present. Its ETH_HLEN wrappers - __vlan_insert_tag() under skb_vlan_push(), and vlan_insert_tag() under validate_xmit_vlan() on the generic transmit path - therefore rewrite the first 16 bytes at skb->data: a 12-byte memmove plus two 2-byte stores at +12 and +14. No caller supplies the bound, while the pop helpers use skb_ensure_writable()/pskb_may_pull(). An IFF_TUN device has hard_header_len == 0, so packet_snd() accepts a one-byte AF_PACKET/SOCK_RAW frame. The first vlan push only sets a hwaccel tag; the next - clsact "action vlan push" or bpf_skb_vlan_push() - enters the helper with skb->len still 1. The head comes from skbuff_small_head without __GFP_ZERO, so each push drags bytes from beyond skb->tail into the frame. After three the one-byte send leaves as 13 bytes carrying 11 bytes of uninitialised slab: 0000: 5a b3 62 12 80 88 ff ff 00 b3 62 12 81 `-----' only 0x5a was sent; the rest is slab, here the top 56 bits of a linear-map address Require the MAC header the helper rewrites to be present, so such a frame is dropped rather than transmitted.	N/A	More Details
CVE-2026-98376	In the Linux kernel, the following vulnerability has been resolved: bpf: Use array_map_meta_equal for percpu array inner map replacement percpu_array_map_ops.map_meta_equal points to the generic bpf_map_meta_equal(), which does not compare max_entries. When a percpu array serves as an inner map, replacing it with one that has fewer max_entries bypasses the check. Since percpu_array_map_gen_lookup() inlines the original template's index_mask as a JIT immediate, a lookup on the replacement map can access pptrs[] out of bounds. Point percpu_array_map_ops.map_meta_equal to array_map_meta_equal(), which already enforces the max_entries equality check. Add a selftest to verify that replacing a percpu array inner map with a differently-sized one is rejected.	N/A	More Details
CVE-2026-98375	In the Linux kernel, the following vulnerability has been resolved: xen/netfront: drop RX packets with a short Ethernet header handle_incoming_queue() pulls pull_to bytes into the head before calling eth_type_trans(). pull_to is the length of the first RX slot, capped at RX_COPY_THRESHOLD, and that length comes from the backend. Nothing checks it against ETH_HLEN. If the first slot is shorter than ETH_HLEN and more slots follow, the head ends up shorter than an Ethernet header while skb->len is longer, and eth_type_trans() BUG()s in __skb_pull(). If the whole packet is shorter than ETH_HLEN, eth_type_trans() reads the header past the end of the data instead. Pull at least ETH_HLEN, and drop the packet if that fails, which also drops packets too short to hold an Ethernet header. This also checks the return value of the pull, which was ignored.	N/A	More Details
CVE-2026-105570	Docker Sandboxes compared OAuth token-endpoint hostnames case-sensitively when deciding whether to mask managed credential responses, while request routing treated DNS hostnames case-insensitively. Untrusted code inside a sandbox could use a case-variant hostname to reach the genuine provider endpoint while bypassing response masking. If a user completed the OAuth flow, the provider's access and refresh tokens could be returned unmasked to the sandbox, exposing host-managed credentials.	N/A	More Details

CVE-2026-4264	Reflected Cross-Site Scripting (XSS) on the BeeTienda e-commerce platform, specifically in the latest demo version. The incident occurs due to a lack of proper sanitization of user input data in the 'search' parameter of the product list endpoint. When malicious payloads are transmitted via the 'search' parameter, they are displayed insecurely in the HTML response, allowing for the arbitrary execution of JavaScript code in the victim's browser.	N/A	More Details
CVE-2026-1907	A SQL Injection (SQLi) affects the Kong Gateway (Enterprise and Open Source) clustering communication logic when operating in Hybrid Mode. The issue can be triggered by sending specially crafted RPC requests to the Control Plane (CP), leading to potential unauthorized database access. Leveraging the issue requires network access to the Control Plane's clustering port and a valid client certificate and key.	N/A	More Details
CVE-2026-107734	SumatraPDF is a multi-format reader for Windows. In 3.5.2 and earlier, an attacker-controlled SyncTeX source filename is substituted for the %f placeholder in an external editor command line without safe Windows argument quoting, and the resulting command line is passed to CreateProcessW(). A user with an external editor configured or auto-detected who opens a PDF with a crafted .synctex.gz file and invokes inverse search can inject command-line flags; the resulting impact depends on the target editor interpreting those flags and can include unintended editor actions or code execution through a malicious extension. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
CVE-2026-108979	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-2026-107386	amqp091-go is a Go AMQP 0.9.1 client. From 1.13.0 until 1.14.0, the frame-size mitigation from the prior allocation advisory can be bypassed before connection.tune completes because Connection.maxFrameSize uses zero for both the not-yet-negotiated and negotiated-unlimited states. A malicious or compromised AMQP peer can send a short body-frame header with a large declared payload length, causing ReadFrame and the body-frame parser to allocate attacker-selected memory before the payload is received or the frame's protocol state is rejected. The condition is reachable through public Open even when Config.FrameSize is set to the protocol minimum and can cause severe memory pressure, out-of-memory termination, or loss of the client process before authentication completes. This issue is fixed in version 1.14.0.	N/A	More Details
CVE-2026-101028	Incorrect Authorization vulnerability in ash-project ash allows an actor to infer data in related records they cannot read via Ash.count/2, Ash.exists/2 and Ash.aggregate/3. Ash.Actions.Aggregate.run/4 (lib/ash/actions/aggregate.ex) applied only the root resource's read policy before running the aggregate query. The read path also applies each related resource's read policy to filter and sort references that cross a relationship, directly (for example comments.body) or through an aggregate over one, but the aggregate path skipped that step. A caller whose filter or sort reaches these functions, for example through Ash.Query.filter_input/2, an ash_lua script, or an AshAi tool offering count or exists results, can test conditions against related rows hidden from them and recover their existence and attribute values one query at a time. Ash.read/2 and its page counts are not affected. This issue affects ash: from 2.6.0 before 3.34.6.	N/A	More Details
CVE-2026-88648	Incomplete X.509 implementation in GnuTLS v3.8.13 allows attackers controlling a subordinate Certificate Authority to bypass cross-domain PKI restrictions and issue unauthorized certificates.	N/A	More Details
CVE-2026-97032	HTTP/2 servers could end up crashing due to inadvertently modifying its HPACK encoder concurrently. This happens because the server modifies the HPACK encoder from two goroutines without synchronization: one uses the encoder to encode a HEADERS frame as part of a response sent to a client and the other modifies the encoder's table size when handling a SETTINGS frame containing SETTINGS_HEADER_TABLE_SIZE that a client sends. A malicious client can repeatedly send a request while changing the header table size to crash the server.	N/A	More Details
CVE-2026-97030	A trusted template author may have previously written a valid template wherein the use of the 'yield' keyword would not be correctly escaped. We now ensure that valid keyword uses are escaped and non-keyword uses are not escaped.	N/A	More Details
CVE-2026-105283	Generation of Error Message Containing Sensitive Information vulnerability in ash-project ash_typescript allows an unauthenticated attacker to read internal Elixir terms from an RPC error response by provoking an error the error builder has no dedicated clause for. AshTypescript.Rpc.ErrorBuilder.build_error_response/1 in lib/ash_typescript/rpc/error_builder.ex renders a pipeline error term that matches no specific clause with inspect/1 and places the result in details.error of the client-facing error. Ash exceptions take a separate path in AshTypescript.Rpc.Errors where unhandled cases are redacted behind an errorId, but these fallbacks have no redaction, so whatever the term carries reaches the HTTP or channel response. Two request paths hand it such terms: a struct-typed action argument with an invalid nested value, where cast_map_to_struct/2 in lib/ash_typescript/rpc/input_formatter.ex throws the raw Ash.Type cast error into the builder, and field selection on a generic action that returns a primitive, where format_field_type/1 inspects the full Ash.Info.Manifest.Type struct into vars.returnType. Resource module names in vars.resource are not treated as sensitive and are out of scope. This issue affects ash_typescript: from 0.1.0 before 0.19.1.	N/A	More Details
CVE-	When a JavaScript template literal contains consecutive expressions, the context tracking state was not		

2026-94448	properly reset upon entering a new expression. We now ensure that template-literal expression entries correctly reset context variables so all subsequent regular expression literals are accurately recognized and escaped.	N/A	More Details
CVE-2026-19396	A predictable seed in the pseudo-random number generator (PRNG) in the IFTTT pairing token generation of the ASUS RT-BE57 router allows an unauthenticated nearby user to derive the pairing token and read or modify router settings via observed values from an administrator-initiated IFTTT pairing session.Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-85499	Improper Authorization vulnerability in Apache SkyWalking BanyanDB. The Canopy includes incomplete proof-of-concept role and monitoring-proxy functionality. Under a non-default configuration with a readonly Canopy user and a reachable monitoring target, that user can send non-read requests through the monitoring proxy. This issue affects Apache SkyWalking BanyanDB: from 0.11.0 before 0.11.1. Users are recommended to upgrade to version 0.11.1, which fixes the issue.	N/A	More Details
CVE-2026-94447	Previously, a user operating inside of a malicious Go project that defines a bogus golang.org/toolchain go.sum entry and operates a malicious GOMODPROXY the user chooses to use can bypass the intended checksum. We now ensure that golang.org/toolchain always goes to the network for the canonical checksum.	N/A	More Details
CVE-2026-94444	Previously, a user operating inside of a malicious Go project that defines a bogus golang.org/fips140 and operates a malicious GOMODPROXY the user chooses to connect to can serve an arbitrary module in its place. We now unpack the trusted ziphash for the bundled golang.org/fips140 module and construct its entry in the GOMODCACHE such that it can be verified by the toolchain.	N/A	More Details
CVE-2026-19572	A security vulnerability has been identified in FlexNet Publisher Imadmin. The vulnerability exists in a SOAP handler, where a hardcoded authentication bypass could allow an unauthenticated user to obtain a privileged administrator session without providing valid credentials.	N/A	More Details
CVE-2026-107735	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, InitializePolicies() starts the sumatrapdfrestrict.ini path with gPolicyRestrictions set to Perm::All and only ORs permission bits, so the INI file never revokes permissions. Deploying SumatraPDF with this INI file, including a malformed file or zero-valued permission settings, can silently bypass configured disk, network, printing, registry, clipboard, preference, and fullscreen restrictions. The -restrict command-line path works correctly and is not affected. No fixed version is available as of this review.	N/A	More Details
CVE-2026-107802	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, src/SelectionTranslate.cpp embeds selected or pasted translation text in quoted Windows command lines using incomplete quote-only escaping. The affected BuildGrokTranslateCmdLineTemp(), BuildClaudeTranslateCmdLineTemp(), and BuildCodexTranslateCmdLineTemp() functions can allow attacker-controlled text to inject model, working-directory, approval, or sandbox-bypass flags when the corresponding agentic CLI backend is installed and used. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
CVE-2026-107738	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, ChmFile::GetCharZ() narrows file-controlled unsigned string offsets from /#WINDOWS and /#IVB to signed integers without a lower-bound check. An offset that becomes negative can make the function read before the /#STRINGS buffer, causing deterministic application termination. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
CVE-2026-107737	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, and in pre-release 3.7.0.20369 when WebView2 is absent or cannot initialize, ParseProtoUrl() accepts the signed host component of an its:// URL and FindHtmlWindowById() uses it directly as an index into gHtmlWindows. Opening a crafted CHM through the IE fallback backend with a negative or otherwise out-of-range window identifier can cause an out-of-bounds pointer read followed by an invalid object callback dereference and process termination. No fixed version is available as of this review.	N/A	More Details
CVE-2026-19386	A stack-based buffer overflow in the ASUS router modules allows an authenticated nearby user to execute arbitrary code via a crafted configuration file upload that exceeds the expected buffer size.Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-107733	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, FrameOnCommand() handles CmdExec by passing a null current-tab pointer to RunWithExe(), which dereferences WindowTab::filePath. A local process in the same interactive Windows session, at an integrity level greater than or equal to SumatraPDF's under Windows UIPI, can dispatch CmdExec over DDE or WM_COPYDATA while no document tab is open, causing abrupt process termination and loss of unsaved state. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject dev-bound-only programs on other devices __bpf_offload_dev_match() falls back to comparing offdev pointers after an exact netdev mismatch. Bound-only programs normally have NULL offdevs, so unrelated netdevs compare equal. A bound-only program on an offload-registered netdev can instead inherit a real offdev and match a sibling port. With CAP_BPF and CAP_NET_ADMIN, a caller can use bpf(BPF_LINK_CREATE) with a different target ifindex to run		

CVE-2026-98382	metadata kfuncs specialized for the bound driver on the target driver's xdp_buff. Running a veth-bound program on tun reads beyond tun's bare stack xdp_buff as a veth_xdp_buff. Oops: general protection fault, probably for non-canonical address KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] RIP: 0010:veth_xdp_rx_timestamp (drivers/net/veth.c:1673) Call Trace: ... tun_build_skb (drivers/net/tun.c:1739) tun_get_user (drivers/net/tun.c:1856) tun_chr_write_iter (drivers/net/tun.c:2091) vfs_write (fs/read_write.c:595 fs/read_write.c:687) ksys_write (fs/read_write.c:739) do_syscall_64 (arch/x86/entry/syscall_64.c:84) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) Kernel panic - not syncing: Fatal exception in interrupt Restrict non-offloaded programs to exact netdev matches and retain the shared-offdev fallback only for genuinely offloaded multi-port programs.	N/A	More Details
CVE-2026-105674	TP-Link Tapo C325WB V2 generates the pre-shared key used by its local media streaming service with a time-seeded pseudo-random number generator, making the key predictable and recoverable. An unauthenticated attacker on the adjacent network can recover the key and authenticate to the media streaming service without valid user credentials. Successful exploitation may allow an unauthenticated adjacent-network attacker to access and take over live video and audio streams, compromising the confidentiality and integrity of camera media.	N/A	More Details
CVE-2026-62171	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-62181	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-107102	This vulnerability exists in the ERP system due to improper validation of payment callback parameters and inadequate authentication controls in API endpoint. An unauthenticated remote attacker could exploit this vulnerability by manipulating the parameter to cause the application to establish an authenticated session for an arbitrary user without valid payment verification. Successful exploitation of this vulnerability could allow the attacker to bypass authentication and gain unauthorized access to other user accounts on the targeted system.	N/A	More Details
CVE-2026-103416	Out-of-bounds write via the TLS 1.3 handshake message cache in NetX Duo in Eclipse ThreadX NetX Duo 6.5.1.202602 allows a handshake message larger than the cache writes past it and on into the rest of the session control block, which holds pointers. A malicious or compromised server can make a TLS 1.3 client produce such a message before certificate authentication completes, so no server certificate is needed to reach it.	N/A	More Details
CVE-2026-102782	Joomla Extension - ordasoft.com - Unauthenticated SQL injection in OrdaSoft Simple Membership < 7.4.0 - site/simplemembership.php dispatches task=checkLoginPass with no authentication or access control check of any kind. The handler reads a login request parameter through Joomla's generic, non-sanitizing input filter, which strips HTML/script tags but never touches quotes or SQL syntax, and concatenates it directly into a query string with no escaping or parameterization:	N/A	More Details
CVE-2026-93858	In OpenStack Mistral through 23.0.0, the std.ssh_proxied action passes a caller-supplied proxy_command value directly to paramiko.ProxyCommand() before any SSH connection to a gateway or target host is attempted. An authenticated project member can use the standard action-execution API to submit an arbitrary local command as proxy_command; paramiko starts that command as a subprocess on the executor host under the executor's own service account, independent of whether the SSH connection itself ever succeeds. Only Mistral deployments that permit the std.ssh_proxied action, the default configuration, are affected.	N/A	More Details
CVE-2026-71884	In Bouncy Castle for Java LTS before 2.73.13, the native one-shot CTR packet cipher did not check that the requested input length fitted the counter space the IV left. In CTR mode the IV and the block counter share one 16-byte block, so an IV of 13 to 15 bytes leaves a counter of only 1 to 3 bytes, addressing 256, 65536 or 16777216 blocks respectively. Given a longer input the counter wrapped and the keystream repeated from the start of the same packet, and the call then returned the full input length as though every byte had been correctly transformed. Two segments of the message were therefore encrypted under the same keystream, so their plaintexts can be recovered from the ciphertext alone, without the key, while the caller saw neither an exception nor a short length to indicate it. The streaming implementation validates at init and again while processing, and the portable AESCTRPacketCipher rejects such a request with "Counter in CTR/SIC mode out of range.", but the native one-shot path has a single entry point and performed no counter-range validation there. It now preflights the IV-derived counter range and rejects an over-long request before any output is written, so the operation is failure-atomic and never reports success for bytes it did not correctly transform. A counter of four bytes or more cannot be exhausted by a Java int length and is unaffected, as is a full 16-byte IV, where the counter range is the caller's responsibility. Bouncy Castle for Java (bcprov) is not affected, as it ships no native implementations.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: sched/cache: Decouple sched_cache_group from mm to fix UAF Currently the sched cache grouping is by mm and the scheduling statistics		

CVE-2026-98385	sched_cache_stat lives in the mm structure. This ties the life cycle of scheduling stats with mm. In account_mm_sched(), the scheduling stats are accessed by task->mm->sc_stat. However, a task may be switching mm on one CPU when another CPU is running account_mm_sched(), and possibly accessing the old mm that was freed. This problem was found when running tests with KASAN by Hyunwoo: https://lore.kernel.org/lkml/apPb-Dr4nPYuHQOK@v4bel/ Instead of serializing the mm access by introducing extra acquisition of rq lock in the mm free path, extract sched_cache_stat from mm_struct, rename it as sched_cache_group and manage its life cycle apart from mm_struct with its own ref counting. This allows us in the next patch access sched_cache_group directly from task, and add a refcount on sched_cache_group when a task links to it. This prevents the use after free issue when accessing stale and released old mm and its sched cache stat a task switches to a new mm while account_mm_sched() is done elsewhere. The other benefit of this restructure is in the future, the grouping of tasks to a LLC would have the flexibility to be associated with a user defined grouping, or cgroup, cookie group, numa_group or others instead of just with a single mm address space. Rename sched_cache_stat to sched_cache_group and turn it into a refcounted object allocated from mm_struct. The mm_struct now holds a pointer (sched_cache_grp) to this object instead of embedding it.	N/A	More Details
CVE-2026-102781	Joomla Extension - ordasoft.com - Unauthenticated Destructive CRUD in OrdaSoft Touch Slider < 5.4.6 - modOsTouchSliderHelper::getAjax(), wired through Joomla's core com_ajax dispatcher, is the single handler behind every data-management operation this module exposes. No call to JFactory::getUser(), authorise(), or a CSRF token check exists anywhere in the handler. Two confirmed impact paths: an unauthenticated GET deletes any slider image by guessable sequential IDs, and an unauthenticated multipart upload with a zip file renames and replaces the entire #__os_touch_slider/#__os_touch_slider_text tables site-wide with attacker-supplied content, with no task parameter even required for the second path.	N/A	More Details
CVE-2026-100197	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-105672	TP-Link Tapo C325WB V2 contains an unauthenticated authorization bypass vulnerability in the HTTPS JSON API dispatcher on TCP port 443. An attacker on the adjacent network can append an onboarding-scoped object to a JSON request to bypass session verification and invoke privileged actions without authentication. Successful exploitation may allow an unauthenticated adjacent-network attacker to access live video and audio, modify device settings, and obtain sensitive device information or secrets.	N/A	More Details
CVE-2026-105673	An unauthenticated denial-of-service vulnerability exists in Tapo C325WB v2 in the RTSP streaming service on TCP port 554 when the Camera Account feature is enabled. A crafted pair of RTSP-over-HTTP tunneling requests can cause memory corruption and crash the streaming daemon. Successful exploitation may allow an unauthenticated adjacent-network attacker to disrupt live video and related streaming functions until the affected service recovers or restarts.	N/A	More Details
CVE-2026-14911	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") in ASUS router modules allows a remote attacker to read DOM information, modify router settings, and cause a denial-of-service condition when an authenticated user visits a crafted URL.Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-93860	In OpenStack Mistral through 23.0.0, the /v2/maintenance API controller clears the request context and calls the maintenance service directly without any policy enforcement. Any holder of a valid Mistral token, regardless of assigned role, can read and change the service's cluster-wide maintenance state. Setting the state to PAUSED stops processing of new workflow and execution objects across all tenant projects until an operator restores it.	N/A	More Details
CVE-2026-98383	In the Linux kernel, the following vulnerability has been resolved: bpf: Disallow bpf_skb_pull_data() for LWT_SEG6LOCAL An LWT_SEG6LOCAL program can invalidate its cached SRH with bpf_lwt_seg6_adjust_srh() and then call bpf_skb_pull_data(). The latter may reallocate skb->head, leaving the per-CPU SRH pointer dangling. Post-program SRH validation then writes through that pointer. Disallow bpf_skb_pull_data() for LWT_SEG6LOCAL programs so the verifier rejects this unsafe helper combination. Other LWT program types continue to expose the helper through lwt_out_func_proto().	N/A	More Details
CVE-2025-64392	This vulnerability in Veeam Backup Enterprise Manager allows an attacker to execute script in the browser of a portal user who opens a crafted link.	N/A	More Details
CVE-2026-16528	Insertion of Sensitive Information into Log File in certain ASUS router models allows a remote authenticated attacker to obtain DDNS credentials from the system log, potentially enabling modification of DNS settings.Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-93861	In OpenStack Mistral through 23.0.0, the workflow membership API lets a project that has accepted a share of another project's private workflow create a further membership naming a third project. The new membership row is created with its project_id defaulted to the accepting project rather than the original workflow owner, and thus the owner can neither see nor delete it. The third project can accept this membership (that it had not actually been granted by the owner), and then read and execute the owner's private workflow; only the	N/A	More Details

	accepting (not the owning) project can later revoke that access.		
CVE-2026-97147	In OpenStack Mistral through 23.0.0, several of the v2 API write paths resolve the target object with a query that can return another project's resource, then write to it. An authenticated project member can use this to rewrite and un-publish another project's public action definitions and environments. A project administrator can create a workbook whose embedded ad-hoc action or workflow name collides with a resource of another project, which moves that resource into the caller's project and causes the original owner's subsequent updates of it to fail with server errors. Only deployments exposing the Mistral API are affected.	N/A	More Details
CVE-2026-101998	Docker Sandboxes could fail open while masking credentials in protected proxy responses. When a response-body read returned data together with an error, affected handlers could forward unmasked bytes. Code inside an authorized sandbox could use this to recover host-managed OAuth access and refresh tokens or a derived Anthropic API key intended to remain outside the sandbox.	N/A	More Details
CVE-2025-64391	This vulnerability in Veeam Agent for Microsoft Windows allows a low-privileged local user to make the agent write files to arbitrary locations when an administrator installs it.	N/A	More Details
CVE-2026-105452	Docker Sandboxes could forward a client-supplied credential alongside a credential injected by the host egress proxy. The proxy removed alternate credentials only when their values matched known sentinel values, so untrusted code in an authorized sandbox could supply an unrecognized credential in another supported authentication header. For affected upstream services, this could authenticate the request to an attacker-controlled account and expose data included in the request.	N/A	More Details
CVE-2026-97853	Memory Allocation with Excessive Size Value vulnerability in ericmj decimal allows Denial of Service. Decimal.round/3 builds the full result for the requested number of decimal places before the context precision (34 digits by default) is applied, so its cost grows with the places argument instead of with the size of the result. For positive places it appends places zero digits to the coefficient as a charlist before converting it to an integer, and for negative places it builds a charlist of -places zero digits. A single call such as Decimal.round(Decimal.new("1.5"), -50_000_000) allocates about 5.5 GB of memory, which can exhaust available memory and get the BEAM VM killed. The oldest releases instead loop once per decimal place, consuming CPU in proportion to places. Any application that passes a user-supplied number of decimal places or scale to Decimal.round/2 or Decimal.round/3 without bounding it is exposed. The input limits added for CVE-2026-32686 do not cover the places argument. This issue affects decimal: from 0.1.0 before 3.1.2.	N/A	More Details
CVE-2026-102368	Affected Tapo device firmware stores device-specific cryptographic material in plaintext within nonvolatile storage. An attacker with physical access to an affected device can recover this sensitive material from the firmware. Successful exploitation of this vulnerability may result in the disclosure of device-specific cryptographic material and could, under certain conditions, increase the risk of unauthorized access to related protected information or communications.	N/A	More Details
CVE-2026-104635	Uncontrolled Recursion vulnerability in Protobuf.JSON.Decode in elixir-protobuf protobuf allows an unauthenticated remote attacker to crash the decoding process via a deeply nested JSON document. Any application that decodes attacker-supplied JSON with Protobuf.JSON.decode/3, Protobuf.JSON.decode!/3, or Protobuf.JSON.from_decoded/3 into a schema that contains a self-referential or cyclic message type is affected. In lib/protobuf/json/decode.ex, the embedded-message clause of decode_singular/3 recurses into internal_from_json_data/3 once per nesting level without incrementing or checking the decoder's depth counter. The depth_guard increase_depth_and_maybe_throw/1 covers only the Google.Protobuf.ListValue and Google.Protobuf.Struct clauses, so the recursion_limit option has no effect on user-defined message types. Each nesting level allocates a stack frame and heap objects, and a sufficiently deep document exhausts the memory of the decoding process. Confidentiality and integrity are not affected. This issue affects protobuf: from 0.8.0 before 0.17.1.	N/A	More Details
CVE-2026-78384	CompressionUtils.inflate() decompressed attacker-controlled DEFLATE data with no output-size cap. A small (~KB) crafted payload could expand to gigabytes on the heap. Reachable via JWE decryption when zip=DEF (e.g. JoseSessionTokenProvider with RSA-OAEP key wrap) and via SAML redirect/POST binding token inflation — in both cases decompression happens before/independent of trust validation. Fix: Added a configurable maximum inflated-size cap (default 10 MiB, org.apache.cxf.compression-max-inflated-size system property) to CompressionUtils.inflate(); aborts with DataFormatException once exceeded. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-107732	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, untrusted document paths and PDF link targets are interpolated into notification text that ParseTip() interprets as trusted tip markup. When a user clicks an injected link, ExecuteTipLink() dispatches its CmdExec command and can execute an attacker-selected local program in the user's context. No broader impact is claimed beyond the advisory-supported conditions. No fixed version is available as of this review.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix out-of-bounds read of sk_protocol in bpf_sock_destroy() sk_protocol lives in struct sock, not in struct sock_common. A timewait or request sock handed to bpf_sock_destroy() by the tcp iterator is neither, so reading sk->sk_protocol runs past the object: =====BUG: KASAN: slab-out-of-bounds in bpf_sock_destroy+0xc7/0xe0 Read of size 2 at addr ffff8881047d11b4 by		

CVE-2026-98384	task test_progs/428 Tainted: [W]=WARN Call Trace: <TASK> dump_stack_lvl+0x91/0xf0 print_report+0xd1/0x630 kasan_report+0xf3/0x130 __asan_report_load2_noabort+0x14/0x30 bpf_sock_destroy+0xc7/0xe0 bpf_prog_c3dd61f9d9cd9f37_iter_tcp6_timewait+0x9f/0xb7 bpf_iter_run_prog+0x538/0xde0 bpf_iter_tcp_seq_show+0x26b/0x4b0 bpf_seq_read+0x424/0x1210 vfs_read+0x197/0xe40 ksys_read+0x119/0x240 __x64_sys_read+0x72/0xc0 x64_sys_call+0x647/0x27e0 do_syscall_64+0xe5/0x610 entry_SYSCALL_64_after_hwframe+0x76/0x7e Only check sk_protocol on full socks. tcp_abort() already knows how to deal with TIME_WAIT and NEW_SYN_RECV socks. Also fix the comment, it never matched the code.	N/A	More Details
CVE-2026-73179	Improper enforcement of single-use authorization code semantics in the JPA OAuth2 authorization code grant provider in Apache CXF allows a remote attacker to obtain multiple valid access tokens from a single authorization code via concurrent token exchange requests that race the non-atomic find-then-delete operation against a shared relational database under READ_COMMITTED isolation. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fixes this issue.	N/A	More Details
CVE-2026-105824	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-79650	Apache CXF's OIDC relying-party component could redirect users to an attacker-controlled URL after successful authentication. The issue occurs because attacker-controlled state parameters are preserved and later used as redirect targets without validating that the final decoded URI belongs to the RP's origin. Both directly encoded and double-encoded external URLs can trigger the issue, depending on which validation path is used. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-4894	A vulnerability has been identified regarding insufficient validation in the Frappe Cloud/ERPNext authentication process, which allows multiple email addresses to be accepted by manipulating the email field in the /api/method/press.api.account.signup endpoint. The vulnerability occurs when an unauthenticated remote attacker adds more than one email address. The service processes the entire value as a valid list of recipients and sends the OTP code to all addresses without proper validation of all added emails (only one of them needs to be valid). Exploiting this vulnerability would allow an attacker to: * Obtain the authentication OTP; * Impersonate someone else in the registration process; * Register accounts using other people's email addresses without access to the mailbox; * Indirectly confirm the existence of already registered email addresses.	N/A	More Details
CVE-2026-5047	A vulnerability in Brocade SANnav before 2.4.0b and 3.0.0 prints encoded passwords and authentication tokens in log files. The vulnerability could allow an authenticated attacker with access to the log file including the SANnav supportsave to access the passwords.	N/A	More Details
CVE-2026-107279	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. In 3.0.12, a peer offering only Digest qop=auth-int causes mutual-authentication verification to be skipped. AuthenticatorUtils.computeExpectedRspAuth returns no expected value for auth-int, and Interceptors treats that result as unverifiable but nonfatal, so a response with an invalid rspauth value is accepted. A peer that does not know the shared secret can therefore be accepted as the authenticated server. This issue is fixed in version 3.0.13.	N/A	More Details
CVE-2025-70515	The device log component of Fanvil x7a firmware version 2.6.0.1182 does not properly sanitize or encode reflected user supplied data. The lack of sanitization allows for the injection of HTML which can be used to execute malicious JavaScript code on any target browser which renders the device log component.	N/A	More Details
CVE-2025-70520	The websocket handler of Fanvil x7a firmware version 2.6.0.1182 does not enforce proper authentication restrictions against sessionless users. The lack of restrictions grants anyone the ability to view any device resources such as operational logs or perform diagnostic requests.	N/A	More Details
CVE-2026-107280	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.13 and 2.16.1, ThreadSafeCookieStore validates Domain attributes with domain matching but does not reject public suffixes. A host beneath a suffix such as co.uk can set a cookie for that suffix, after which the shared cookie store sends it to unrelated hosts under the suffix. This can inject or overwrite session-relevant cookie values across origins. This issue is fixed in versions 3.0.13 and 2.16.1.	N/A	More Details
CVE-2026-107281	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.13 and 2.16.1, the HTTP/1.1 connection-pool key excludes the authenticated principal for connection-oriented NTLM and Negotiate authentication. A pooled socket authenticated for one request can be reused by a request carrying another principal, and the server executes that later request as the first identity. Basic and Digest are not affected because they authenticate each request. This issue is fixed in versions 3.0.13 and 2.16.1.	N/A	More Details
CVE-2026-94587	A buffer overflow vulnerability exists in the WebTools administrative interface handling configuration download or file transfer operations of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An authenticated user with permissions to perform configuration downloads using remote server profiles can overflow stack buffers causing a crash of the weblinker daemon.	N/A	More Details

CVE-2026-94586	A command injection vulnerability exists in the WebTools administrative interface handling configuration download or file transfer operations of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An authenticated user with permissions to perform configuration downloads using remote server profiles can supply malicious parameter strings to execute arbitrary shell commands on the switch with root privileges	N/A	More Details
CVE-2026-94585	An authentication bypass vulnerability exists in the web management interface of Brocade Fabric OS versions before 9.2.2d running on the MXG610 platform. An unauthenticated, network-adjacent attacker can exploit an unauthenticated endpoint within the Single Sign-On (SSO) workflow to gain administrative access to the device management interface.	N/A	More Details
CVE-2026-94581	An OS command injection vulnerability exists in the REST API management interface of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1 allows an authenticated, high-privileged remote attacker to execute arbitrary system commands with root permissions. An attacker with administrative privileges to configure SSH known host settings can supply specially crafted parameter values containing shell metacharacters to trigger command execution on the host system.	N/A	More Details
CVE-2026-94579	An OS command injection vulnerability exists in the PAM (Pluggable Authentication Module) session cleanup routines during SSH session termination on Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An authenticated user authenticating via an external directory or AAA service whose username or profile identifier contains shell metacharacters can trigger arbitrary command execution with root privileges when their remote SSH session closes.	N/A	More Details
CVE-2026-94577	A privilege escalation vulnerability exists in the internal Command-Line Interface (CLI) authorization handling mechanism of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An authenticated user or local process that can manipulate the process execution environment can bypass Role-Based Access Control (RBAC) validation checks. Successful exploitation allows an attacker to elevate privileges to root	N/A	More Details
CVE-2026-94576	An authentication logic and privilege escalation vulnerability exists in the account management interface of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. Under specific conditions, an authenticated user can bypass authorization restrictions intended to prevent modifying another account's access privileges. Exploitation allows a lower-privileged user to assign administrative roles to a target account, leading to localized privilege escalation.	N/A	More Details
CVE-2026-87677	An OS command injection vulnerability exists in the account management subsystem of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When an administrator initiates an account deletion, the system invokes an internal maintenance routine to clean up cryptographic keys associated with the target account. Malformed account names previously accepted by Fabric OS can cause the execution of embedded shell metacharacters, triggering command injection.	N/A	More Details
CVE-2026-87664	A session context forgery vulnerability exists in the web management daemon of Brocade Fabric OS versions 9.2.2d and 10.0.0 through 10.0.0a1. When processing local inter-process communication (IPC) storage callbacks, the service accepts and registers session structures including administrative role permissions, user identifiers, and authorization flags—without verifying the identity or authenticity of the sending process. An attacker can obtain elevated administrative privileges on the web management interface without legitimate authentication.	N/A	More Details
CVE-2026-103501	Heap buffer overflow in the HLL sketch deserialization of Apache DataSketches C++ (repo: datasketches-cpp). When deserializing a sketch in LIST mode, from either a byte buffer or a stream, the coupon count was read from the input and used as the number of entries to copy into a fixed buffer of 8 entries, without checking it against the buffer's capacity. A crafted sketch could cause a write of up to 988 bytes past the end of this internal heap buffer. This can corrupt heap memory, causing a crash and potentially enabling further exploitation. This issue affects Apache DataSketches C++: from 1.0.0-incubating before 5.3.0. Only applications that deserialize HLL sketches from untrusted sources are affected. Users are recommended to upgrade to version 5.3.0, which fixes this issue.	N/A	More Details
CVE-2026-103513	Out-of-bounds read and write in the CPC sketch deserialization of Apache DataSketches C++ (repo: datasketches-cpp). A crafted serialized CPC sketch passed to cpc_sketch::deserialize(), from either a byte buffer or a stream, can cause the decompressor to read past the end of the compressed data, because the read position was only checked after decoding finished. In the hybrid flavor, it can also cause a write outside an internal heap buffer, because decoded row indices were not validated. Several other header fields and decoded values, including lg_k, were also not validated. This can corrupt heap memory, causing a crash and potentially enabling further exploitation. This issue affects Apache DataSketches C++: from 2.0.0-incubating before 5.3.0. Only applications that deserialize CPC sketches from untrusted sources are affected. Users are recommended to upgrade to version 5.3.0, which fixes this issue.	N/A	More Details
CVE-2026-5048	In Brocade SANnav before 3.0.0a, an SQL Injection vulnerability in various external API inventories have a vulnerability that allows an authenticated attacker to inject malicious data into some of the REST API -query parameters.	N/A	More Details
CVE-2026-	A path traversal vulnerability affects the The Zone Alias Import flow feature in Brocade SANnav before 3.0.0a. A local authenticated attacker can write an uploaded content outside the intended directory.	N/A	More Details

5049			
CVE-2026-5769	A vulnerability in Brocade SANnav before 3.0.1 can have the Brocade Fabric OS switch admin password captured in plaintext within a memory swap file on the server hosting the Brocade SANnav Virtual Machine (VM). This can happen when the SANnav server encounters an Out Of Memory (OOM) condition. The vulnerability could allow an authenticated admin user with access to the server hosting the SANnav to potentially view the memory swap file and access the password(s).	N/A	More Details
CVE-2026-85490	When Brocade ASCG before 3.5.0 processes support bundle archives ingested from remote compromised endpoints, the application fails to sanitize path traversal sequences contained within archive entries prior to extraction. An unauthenticated remote attacker capable of sending or intercepting ingested archive files can leverage this flaw to write arbitrary files to restricted locations on the underlying host, potentially leading to remote code execution.	N/A	More Details
CVE-2026-98373	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: preserve mremap address delta when skipping page tables move_hugetlb_page_tables() optimizes mremap() by advancing to the last entry in the page table when the source page table does not exist, either initially or after unsharing a PMD table. The common loop increment then steps to the first entry in the next page table. However, the code advances both the source and destination addresses to the last entries in their respective page tables, which is wrong. The destination address must be advanced only by the same amount as the source address. If the source and destination offsets within their page tables differ, the destination address can be advanced too far, causing follow-up issues. Fix this by advancing the destination address by the source advance distance. With a reproducer, we were able to trigger a kernel panic on x86-64. With this fix in place, we can no longer reproduce the issue.	N/A	More Details
CVE-2026-93699	Argument injection in WP Toolkit for cPanel allows local users to execute arbitrary code as other accounts on the same server.	N/A	More Details
CVE-2026-98374	In the Linux kernel, the following vulnerability has been resolved: tcp: fix use-after-free of retransmit_skb_hint in tcp_send_synack() When tcp_send_synack() replaces the cloned SYN skb at the head of the retransmit queue with a copy, it frees the original with tcp_rtx_queue_unlink_and_free() and only repairs tp->highest_sack. tp->retransmit_skb_hint keeps pointing at the freed skbuff_fclone_cache object. The dangling hint is read in tcp_verify_retransmit_hint() and used as the root of the rbtree walk in tcp_xmit_retransmit_queue(). An unprivileged TFO client (sendmsg(MSG_FASTOPEN)) can arm the hint with an attacker-supplied ICMP fragmentation-needed message, after which a simultaneous open frees the armed SYN skb: BUG: KASAN: slab-use-after-free in tcp_mark_skb_lost (net/ipv4/tcp_input.c:1316) Read of size 4 at addr ffff88800604d928 by task swapper/1/0 Call Trace: tcp_mark_skb_lost (net/ipv4/tcp_input.c:1316) tcp_simple_retransmit (net/ipv4/tcp_input.c:3158) tcp_v4_err (net/ipv4/tcp_ipv4.c:587) Sync the hint to the copy.	N/A	More Details
CVE-2026-87428	In Brocade ASCG before 3.5.0, a local unauthorized user on the ASCG VM who can issue a request to the SANnav host network namespace can extract stored management credentials for onboarded SANnav instances and compromise connected Brocade SANnav servers or managed Brocade Fibre Channel switches.	N/A	More Details
CVE-2026-87426	An unauthenticated network-based attacker can query specific internal management endpoints on Brocade ASCG versions before 3.5.0 to enumerate the configuration details and state of managed Brocade Fabric OS (FOS) switches. This results in the unauthorized disclosure of the customer's SAN fabric management topology and switch connectivity attributes.	N/A	More Details
CVE-2026-87425	An unauthenticated remote attacker can modify the TLS client trust store in Brocade ASCG versions before 3.5.0. By supplying an unauthorized Certificate Authority (CA) certificate to an unauthenticated management interface, the attacker can cause the system to trust unauthorized certificates, potentially enabling Man-in-the-Middle (MITM) attacks against outbound communications with managed switches and peer nodes.	N/A	More Details
CVE-2026-87424	A vulnerability in the SupportLink API authentication component of Brocade ASCG versions prior to 3.5.0 allows an attacker to bypass authentication across deployments due to the use of a hard coded cryptographic key.	N/A	More Details
CVE-2026-85489	An authentication flaw exists in the Brocade ASCG administrative management service component. An unauthenticated network user can issue direct API requests to perform privileged actions, including accessing sensitive system configuration mapping data, modifying managed device inventories, and altering operational settings. This vulnerability affects all versions of Brocade ASCG before 3.5.0.	N/A	More Details
CVE-2026-107231	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.13 and 2.16.1, Realm.Builder treats a Digest challenge that yields no usable nonce as a Basic challenge. A malicious origin or proxy can label a challenge Digest while omitting or emptying the nonce, causing the client to resend the username and password using reversible Basic authentication. Both origin and proxy challenge parsers are affected. This issue is fixed in versions 3.0.13 and 2.16.1.	N/A	More Details
	Brocade ASCG before 3.5.0 has a well-known Brocade default password embedded in a script distributed to		

CVE-2026-85488	every customer. Any local authenticated user with read access to the installation path can discover this credential and perform privilege escalation on affected Open Virtual Appliance (OVA) deployments, where default configuration settings remain in place.	N/A	More Details
CVE-2026-85487	A path traversal vulnerability exists in the HTTP service component of Brocade ASCG versions before 3.5.0. An unauthenticated attacker on the local network could send a manipulated API request to the service endpoint bypassing path restrictions to arbitrary file read, file write, or file deletion operations.	N/A	More Details
CVE-2026-107194	Sungrow iSolarCloud before 2026 allows authentication bypass and account takeover via "login_type": "5" in a login request, potentially leading to "local blackouts on the whole continent" in Europe. An email address for the user_account property is required; however, a user can view the email address associated with their parent organization.	N/A	More Details
CVE-2026-85486	Brocade ASCG before 3.5.0 improperly processes user input by evaluating form data prior to validation. When an authenticated user submits a configuration form, the submitted text could immediately be processed. A malicious actor with basic access can supply crafted input to execute arbitrary code on the server and take control of the application.	N/A	More Details
CVE-2026-85423	A vulnerability has been identified in the data collection service of Brocade ASCG versions before 3.5.0. An API endpoint within the data collector service fails to perform authentication or authorization checks on incoming requests. An attacker with network access to the service can instruct the application to establish SSH connections to arbitrary hosts and execute arbitrary system commands, effectively turning the appliance into an unauthenticated proxy or execution vector.	N/A	More Details
CVE-2026-85422	A vulnerability in Brocade ASCG version before 3.5.0 could allow an attacker to obtain a static cryptographic key hardcoded into the software binaries to secure sensitive data at rest and to protect inter-node communication protocols. An attacker who extracts this key can decrypt stored management credentials or craft forged administrative synchronization messages.	N/A	More Details
CVE-2026-85421	A critical security vulnerability has been identified in Brocade ASCG versions before 3.5.0. The HTTPS service fails to properly enforce authentication or access control checks on incoming requests. An unauthenticated attacker with network access can issue control commands, alter cluster states, and modify system configurations, leading to a complete compromise of the streaming service control plane.	N/A	More Details
CVE-2026-103635	Out-of-bounds read in the compact Theta sketch deserialization of Apache DataSketches C++ (repo: datasketches-cpp). compact_theta_sketch::deserialize() and wrapped_compact_theta_sketch::wrap() read header fields before checking that the input was long enough. For the compressed format, the size check could be defeated by a 32-bit overflow, and two header fields that control decoding were not validated; this also affected deserialization from a stream. A crafted or truncated sketch could cause a read past the end of the input. In the compressed case the over-read can be large, and the bytes read can become part of the deserialized sketch. This can cause a crash (denial of service) and could expose adjacent memory contents. This issue affects Apache DataSketches C++: from 3.1.0 before 5.3.0. Only applications that deserialize Theta sketches from untrusted sources are affected. Users are recommended to upgrade to version 5.3.0, which fixes this issue.	N/A	More Details
CVE-2026-103636	Out-of-bounds read in the VarOpt union deserialization of Apache DataSketches C++ (repo: datasketches-cpp). var_opt_union::deserialize() read the 32-byte preamble of a non-empty union after checking that only 8 bytes were available, so a truncated serialized union could cause a read of up to 24 bytes past the end of the input. For such inputs, the size remaining for the embedded sketch was also computed by an unsigned subtraction that could wrap around, so the embedded sketch's own size checks no longer limited reads to the input. The bytes read can become part of the deserialized union's state. This can cause a crash (denial of service) and could expose adjacent memory contents. This issue affects Apache DataSketches C++: from 2.0.0-incubating before 5.3.0. Only applications that deserialize VarOpt unions from untrusted sources are affected. Users are recommended to upgrade to version 5.3.0, which fixes this issue.	N/A	More Details
CVE-2013-10076	ExtUtils::Typemaps::STL::Vector versions before 1.05 for Perl allocate a 32 GiB array on an empty list. The OUTPUT typemaps call av_extend(av, len-1). On an empty list, this undeflows, and av_extend will allocate an array with 2^32 slots, leading to memory exhaustion.	N/A	More Details
CVE-2026-94578	Brocade Fabric OS versions before 10.0.1 contain an authorization logic vulnerability in the AAA (Authentication, Authorization, and Accounting) integration framework allows remote authenticated users to gain root-equivalent chassis access controls. By returning specific, crafted Vendor-Specific Attributes (VSAs) or directory claims from an external identity provider (such as RADIUS, LDAP, TACACS+, or Federated IDP), an account can bypass administrative role restriction checks during session establishment.	N/A	More Details
CVE-2026-107276	MISP contains a race condition in the email-based one-time password (OTP) login flow. When two HTTP requests carrying the same valid OTP are submitted concurrently, both can successfully authenticate and establish a session. The root cause is that the OTP value is read from the shared store, validated, and then deleted in separate non-atomic steps, allowing a second in-flight request to read the same value before the first request's deletion takes effect. Preconditions: - The target MISP instance has email OTP login enabled. - The attacker possesses a valid, unexpired OTP (e.g., via email interception or social engineering). - The attacker can issue two HTTP POST requests in close temporal proximity. Impact: - The one-time-use	N/A	More Details

	guarantee of the OTP is violated; a single code can yield two authenticated sessions. - This weakens the authentication control and may facilitate unauthorized access if the OTP is shared or intercepted. Affected versions: <2.5.48		
CVE-2026-107278	MISP contains a validation flaw in its object synchronization logic. When a MISP Object is created without a description, it is stored correctly on the originating instance. However, when that object is replicated to another MISP instance via the sync mechanism, the receiving instance's validation rule rejects the object because the description field is empty. As a result, the receiving instance silently drops the object along with all of its associated attributes, leading to loss of threat-intelligence data. Preconditions: - Two or more MISP instances are configured to synchronize objects. - A user with object-creation privileges creates an object without supplying a description. - The object is subsequently synced to a peer instance. Impact: - Valid objects and their attributes are silently discarded on receiving instances, causing data-integrity loss in the threat-intelligence pipeline. - The issue is not externally exploitable in a traditional sense but can be triggered by any authorized user who creates objects without descriptions, resulting in unintended data loss across the sync topology. Affected: <2.5.48.	N/A	More Details
CVE-2026-33586	Authenticated users are able to manipulate both the SMTP envelope "Envelope-from" and "From" fields when sending emails through OVH mail servers. Due to OVH's default SPF configuration, which commonly includes include:mx.ovh.com, any authenticated user with a valid OVH email account can send messages that appear to originate from any OVH-hosted domains using the default SPF record. Since the SPF policy explicitly authorizes OVH mail servers (mx.ovh.com) to send mail on behalf of these domains, forged messages successfully pass SPF validation despite not being authorized by the impersonated domain owner.	N/A	More Details
CVE-2026-107406	Memory overflow vulnerability leading to Remote Code Execution or Denial of Service Vulnerability in NetScaler ADC. NetScaler ADC or NetScaler Gateway must be configured as a SAML SP or SAML IdP, subject to the following version-specific requirements: * For the following versions: Applicable only when configured as a SAML IdP: * NetScaler ADC and NetScaler Gateway between 14.1-73.37 and 14.1-73.41, inclusive * NetScaler ADC 14.1-FIPS between 14.1-73.37 FIPS and 14.1-73.41 FIPS, inclusive * NetScaler ADC and NetScaler Gateway between 13.1-64.23 and 13.1-64.28, inclusive * NetScaler ADC 13.1-FIPS between 13.1-NDcPP 13.1-37.279 and 13.1- 37.282, inclusive For the following versions: Applicable only when configured as a SAML SP or SAML IdP: * NetScaler ADC and NetScaler Gateway before 14.1-73.37 * NetScaler ADC 14.1-FIPS before 14.1-73.37 FIPS * NetScaler ADC and NetScaler Gateway before 13.1-64.23 * NetScaler ADC 13.1-FIPS before13.1-NDcPP 13.1-37.279	N/A	More Details
CVE-2026-94583	A race condition vulnerability exists in the request processing logic of the REST management interface on Brocade Fabric OS versions before 10.0.1. When handling concurrent incoming network management FCIP requests, a timing window exists between when a request populates the address variable and when the service constructs and returns the response context. As a result, the first request adopts the modified context, causing the service to return sensitive management details or configuration data belonging to the second context back to the original requester.	N/A	More Details
CVE-2026-94582	A memory buffer overflow vulnerability exists in the internal diagnostic and route validation routines used by the Fabric Shortest Path First (FSPF) protocol component of Brocade Fabric OS versions before 10.0.1. While this code path is part of internal diagnostic functionality and is not directly accessible via standard user interfaces or CLI management commands, an input processing flaw allows incoming or internally routed diagnostic state payloads to exceed allocated memory boundaries. An attacker that is able to chain or link other vulnerabilities to exploit this internal diagnostic could cause a heap- or stack-based memory overrun, resulting in a daemon crash (Denial of Service) or potential arbitrary code execution within the context of the routing daemon.	N/A	More Details
CVE-2026-104841	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-97664	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-103357	Missing Authorization vulnerability in VillaTheme GIFT4U gift4u-gift-cards-all-in-one-for-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GIFT4U: from n/a through 1.1.3.	N/A	More Details
CVE-2026-102488	In affected versions, Octopus Server incorrectly evaluates multiple scoped permission assignments, allowing a highly privileged user to obtain deployment permissions beyond those actually granted to them.	N/A	More Details
CVE-2026-92862	The Android application "Ticket Ryutsu Center" improperly handles custom URL schemes, allowing a malicious application to cause access to an arbitrary website via a crafted Intent.	N/A	More Details
CVE-2026-	The Android application "Ticket Ryutsu Center" contains hard-coded credentials, which may allow an attacker	N/A	More

92861	to obtain an API key used by the application.		Details
CVE-2026-87686	An authentication and access control bypass vulnerability exists in the web server management interface of Brocade Fabric OS versions before 10.0.1. The web dispatcher routine evaluates internal management VLAN trust decisions using the client-supplied HTTP host header instead of the actual socket transport layer source IP address. Successful exploitation allows the attacker to bypass IP-filtering access control lists (ACLs) and obtain sensitive device metadata (such as model, serial number, hardware revision, and firmware version) without authentication.	N/A	More Details
CVE-2026-87684	A stack-based buffer overflow vulnerability exists in the SNMP daemon request handling of Brocade Fabric versions before 10.0.1. When processing an incoming SNMPv3 packet, an internal statistics gathering handler copies user-supplied context name data into a fixed-size buffer without properly validating the length of the string. A remote, unauthenticated attacker (under default configuration) can exploit this vulnerability by sending a specially crafted SNMPv3 packet, leading to memory corruption, daemon crash (Denial of Service), or potential arbitrary code execution.	N/A	More Details
CVE-2026-87678	An input validation and output encoding vulnerability exists in the web management interface of Brocade Fabric OS versions before 10.0.1. When configuring Federated Authentication (FA), the system fails to sanitize the Identity Provider (IdP) issuer parameter. An authenticated administrator—or an attacker capable of supplying crafted FA configuration files during an import routine—can inject arbitrary web server directives. This can lead to service denial by preventing the web management daemon from starting, or potentially alter web server security controls.	N/A	More Details
CVE-2026-87676	A stack-based buffer overflow vulnerability exists in the security library component of Brocade Fabric OS versions before 10.0.1. When parsing uploaded X.509 PEM certificates for management display, the system improperly validates the length of the Authority Key Identifier (AKI) extension before copying string tokens into an internal memory buffer. An authenticated user with administrative privileges to import custom certificates can supply a certificate containing an intentionally oversized AKI extension. When the system processes or renders the certificate attributes, this can trigger a stack memory corruption leading to a denial-of-service (DoS) condition by crashing the management daemon.	N/A	More Details
CVE-2026-87660	An improper file permission and missing authorization vulnerability exists in the diagnostic kernel module subsystem of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An unprivileged local user can invoke privileged hardware tests, force system error conditions, reset hardware blades, or disrupt storage fabric operations.	N/A	More Details
CVE-2026-87666	An OS command injection vulnerability exists in the time and zone management subsystem of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When updating system timezone settings via the REST API or configuration download routines, the system fails to sanitize input values before processing them in underlying shell execution routines. An authenticated user with low-privilege administrative access can exploit this vulnerability by submitting a crafted timezone string containing shell metacharacters. Successful exploitation allows the attacker to escape the restricted management environment and execute arbitrary shell commands with elevated privileges.	N/A	More Details
CVE-2026-107373	ExtUtils::Typemaps::STL::String versions before 1.06 for Perl T_STD_STRING typemap may read the SV length before stringifying the argument. The typemap uses \$var = std::string(SvPV_nolen(\$arg), SvCUR(\$arg)) However, evaluation order for C++ arguments is not specified, and some compilers may produce code that evaluates SvCUR(\$arg) first. When \$arg is not a string (for example, an integer, number or a reference) then SvCUR will return an invalid value, and the program may abort or segfault.	N/A	More Details
CVE-2026-94584	A race condition and thread-safety vulnerability exists in the web management daemon of Brocade Fabric OS versions before 10.0.1. When handling user authentication requests across a multi-threaded execution pool, this race condition causes PAM modules to process stale or incorrect client IP addresses and switch context numbers. This leads to inaccurate audit records and potential access control bypasses where AAA evaluation or Calling-Station-ID ACL policies rely on client IP attributes.	N/A	More Details
CVE-2026-107794	ExtUtils::Typemaps::STL::List versions before 1.07 for Perl allocate a 32 GiB array on an empty list. The OUTPUT typemaps call av_extend(av, len-1). On an empty list, this undeflows, and av_extend will allocate an array with 2^32 slots, leading to memory exhaustion. Note that a similar issue was fixed in ExtUtils::Typemaps::STL::Vector version 1.05.	N/A	More Details
CVE-2026-87663	An authentication bypass and command injection vulnerability exists in the inter-switch remote execution service of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When processing remote command execution IPC frames across the fabric, the receiving switch processes these commands at an elevated processing level without proper verification of transmitted parameters. This allows an attacker on a single fabric-connected switch to escalate privileges and execute arbitrary root commands locally or across other managed fabric members where remote execution functionality is enabled.	N/A	More Details
CVE-2026-87662	Brocade Fabric versions before 9.2.2d and 10.0.0 through 10.0.0a1 handling of specific download protocols utilizes unsanitized parameter strings. When processing upgrade requests, parameters are converted into system command strings and executed through a system shell interface. Because control characters and shell metacharacters in fields like the host or file path are not stripped or sanitized, an attacker can execute	N/A	More Details

	arbitrary shell commands with the firmware management daemon's elevated privileges.		
CVE-2026-87661	Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1 directly accepts Apache configuration file data during service setup or re-initialization. An attacker capable of corrupting the configuration structure will prevent the web management service from starting or recovering during service bring-up, leading to a persistent Denial of Service (DoS) of the administrative web interface.	N/A	More Details
CVE-2023-5649	An Improper Input Validation vulnerability for the registered case credentials in Brocade ASCG before v3.0 could allow a local authenticated user to provide invalid inputs like special characters leading to a Denial of Service (DoS) when collecting “supportsave” from a Brocade Switch.	N/A	More Details
CVE-2026-107282	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Prior to 3.0.13 and 2.16.1, cross-host request replay updates the current request but leaves the target request and related proxy context pointing at the original origin. Connection-pool selection, CONNECT handling, realm selection, and TLS setup can consequently send the original host's path, Host header, Authorization credentials, or plaintext request to the replay destination. Documented ResponseFilter failover and retry paths can trigger the replay. This issue is fixed in versions 3.0.13 and 2.16.1.	N/A	More Details
CVE-2023-5648	In Brocade ASCG before Brocade ASCG v3.0, several security-related HTTP Headers were missing in various Brocade ASCG URL paths, aiding unauthenticated attackers to perform attacks such as Cross-Site Scripting, Clickjacking, Information disclosure, and more.	N/A	More Details
CVE-2026-94580	An arbitrary file and directory deletion vulnerability exists in the REST API management interface handling USB storage operations on Brocade Fabric OS versions before 10.0.1. An authenticated user possessing USB management privileges can manipulate requested target paths to delete arbitrary files or directories on the switch's local root filesystem, bypassing intended USB mount point boundaries.	N/A	More Details
CVE-2026-87667	An argument injection vulnerability exists in the configuration management command-line utility of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When executing configuration viewing commands with search pattern filters, the utility fails to sanitize user-supplied search string options before passing them to internal search commands. An authenticated user with low-privilege administrative access can exploit this vulnerability to read arbitrary files on the local operating system, including sensitive configuration files, system password hashes and system secrets.	N/A	More Details
CVE-2026-94575	A logic vulnerability in Brocade Fabric OS versions before 10.0.1 web management framework allows an authenticated, low-privileged user to bypass inner Role-Based Access Control (RBAC) checks under specific environmental conditions. Successful exploitation lowers the system authorization mode for the active session context, allowing access to restricted configuration settings intended exclusively for administrative roles.	N/A	More Details
CVE-2026-87688	An input validation vulnerability exists in the security certificate management component of the Brocade Fabric OS administrative management API. When processing certificate management operations, user-supplied certificate identifiers are handled without adequate sanitization prior to execution in external system routines. An authenticated attacker with privileges to perform certificate deletion requests can leverage this flaw to execute arbitrary system commands with the privileges of the underlying management daemon. This vulnerability affects Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1.	N/A	More Details
CVE-2026-87687	An authorization and input validation vulnerability exists in Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. An authenticated user with restricted privileges in one Virtual Fabric can exploit this issue by submitting a specially crafted request containing an arbitrary fabric identifier. This allows the user to perform unauthorized cross-fabric operations and view configuration details within tenants/Virtual Fabrics to which they have not been granted access.	N/A	More Details
CVE-2026-87685	An arbitrary file manipulation vulnerability exists in the WebTools management interface of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When processing configuration transfer requests, the application fails to properly validate and sanitize a user-supplied status file path parameter. An authenticated administrative user can exploit this issue by submitting a specially crafted status file parameter, causing the underlying process to move an arbitrary system file to a predictable, world-readable temporary directory. This can lead to persistent Denial of Service (DoS), critical system file destruction, host compromise, or sensitive data leakage.	N/A	More Details
CVE-2026-87675	An OS command injection vulnerability exists in the configuration management subsystem of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. When performing a configuration download operation, the management daemon will relay configuration parameters, user-supplied relay host strings, and filenames directly to an internal utility script without sufficient character set validation. Because the local utility fails to sanitize shell metacharacters before processing them in a system shell command, a malicious or compromised configuration file can cause arbitrary operating system commands to be executed on a remote local switch when an administrator initiates a configuration download.	N/A	More Details
CVE-	A local privilege escalation vulnerability exists in the system logging daemon of Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. Insufficient access controls on internal inter-process		

2026-87674	communication (IPC) channels allow an unprivileged local user to submit malformed logging configurations. Due to improper input sanitization during configuration file generation, an attacker can inject arbitrary directives that execute with elevated privileges when the logging service reloads, leading to local privilege escalation.	N/A	More Details
CVE-2026-87673	An OS command injection vulnerability exists in maintenance command-line diagnostic utilities on Brocade Fabric OS versions before 9.2.2d and 10.0.0 through 10.0.0a1. The binary fails to sanitize user-supplied input options when invoking underlying system commands through a shell interpreter. A privileged user with maintenance account access can exploit this issue by supplying crafted parameters, which results in arbitrary OS command execution with root privileges.	N/A	More Details
CVE-2026-12260	SQL injection in the NetBoard CRM demo platform; specifically, the vulnerable component is the 'user-name' POST parameter in the '/module/auth/recovery.php' endpoint. The parameter is vulnerable to blind attacks based on Boolean, error, time-based and UNION techniques. Exploitation allows attackers to extract confidential information (such as the version and type of backend used), alter data or further compromise the CRM environment.	N/A	More Details
CVE-2026-107503	Unvalidated environments URL allows OAuth authorization code + PKCE verifier theft and account takeover via injected OIDC authority in Ditto Explorer in Eclipse Ditto Ditto Explorer [3.6.0,3.9.7] allows a craft link set an attacker-controlled OIDC authority with autoSso enabled. The UI then automatically starts a login at the genuine identity provider but exchanges the returned authorization code together with its PKCE code_verifier at an attacker-controlled token endpoint. This lets the attacker redeem the code for the victim's access and refresh tokens. Alternatively, an attacker-controlled api_uri causes the UI to send the victim's bearer token or Basic credentials to the attacker. Because the configuration is persisted, later visits to the UI without the crafted link repeat the token theft.	N/A	More Details
CVE-2026-86463	Apache CXF's FIQL query parser has a vulnerability in how it searches for operators in query expressions. The search pattern can get stuck trying many combinations when it encounters a long string without an operator, causing the parser to consume excessive CPU time. An attacker can send a crafted query to make the server use up CPU resources, potentially slowing down or stopping other requests. The fix was to limit FIQL expressions to 4 KiB by default, preventing attackers from sending extremely long inputs while still allowing normal queries. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-101947	ExifTool for photo and video 5.0.1-gms by CellHubs constructs shell command strings from file paths and invokes /system/bin/sh -c. In the CSV-export path, the selected media path is merely surrounded with single quotes; embedded single quotes are not escaped.	N/A	More Details
CVE-2026-97146	Apache YuniKorn 1.9.0 and earlier allows bypassing the check for the user annotation by setting a secondary label on the pod. If the pod has the label 'app=yunikorn' the checks limiting the user annotation content are not run. The label is used to identify the YuniKorn application itself in the deployments. The bypass allows any user to specify an arbitrary user info annotation. The arbitrary user information could allow access to a queue that the user normally would not have access to. Quota usage for the queue might be impacted if the application runs in the incorrect queue. User based quota enforcement is also based on the user annotation. User quota tracking could be side stepped even if the application runs in the correct queue. Users are recommended to upgrade to version 1.10.0, which fixes this issue.	N/A	More Details
CVE-2026-105826	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-105825	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-103668	An SQL Injection vulnerability exists in the Site Search function of Movable Type, which may allow an unauthenticated attacker to execute an arbitrary SQL query on the affected product.	N/A	More Details
CVE-2026-87672	An information disclosure vulnerability exists in the SupportLink diagnostic collection utilities of Brocade Fabric OS versions before 10.0.1. When SupportLink is configured to use an authenticated HTTP proxy, the system stores the full proxy URL. Anyone with access to the diagnostic support bundle, such as support personnel or users with access to file shares where support bundles are stored, can extract these cleartext proxy credentials.	N/A	More Details
CVE-2026-102916	A reachable assertion in the illumos bhyve instruction emulator allows a guest to panic the host. When emulating a REP-prefixed MOVS or STOS instruction that accesses guest MMIO, vie_emulate_movs() and vie_emulate_stos() in usr/src/uts/intel/io/vmm/vmm_instruction_emul.c do not clear the VIES_REPEAT status flag on the final iteration. For MMIO regions emulated in the kernel (the local APIC, I/O APIC and HPET), the stale flag causes a VERIFY assertion in vie_advance_pc() to fail, and the host panics. A privileged user within a guest VM can issue a REP MOVS or REP STOS instruction against the local APIC page to cause a denial of service of the host and every other guest running on it. The flaw has existed since 2020 (illumos-gate commit e0c0d44e), and affects any illumos distribution prior to illumos-gate commit 696ecf8d.	N/A	More Details

CVE-2026-105823	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-104112	A missing release of resources in the illumos name service cache daemon (nscd) allows a local user to exhaust kernel memory. The nscd door server procedure, switcher() in usr/src/cmd/nscd/nscd_frontend.c, does not close file descriptors that are passed with a door call but not used by the request, and the main nscd door at /var/run/name_service_door accepts passed descriptors from any user in its zone. Because nscd also runs with an unlimited file descriptor limit, an unprivileged local user, including one in a non-global zone, can repeatedly pass a descriptor to its zone's nscd in a door_call() loop, causing the file descriptor table of nscd to grow without bound in kernel memory. This causes a denial of service of nscd and can render processes in all zones on the host unresponsive. The flaw has existed since 2006 (illumos-gate commit cb5caa98), and affects any illumos distribution prior to illumos-gate commit af810a72.	N/A	More Details
CVE-2026-104113	A double free in the IP management daemon (ipmgmt) of OmniOS and SmartOS allows a local user to crash the daemon. When authorizing a door request that modifies interface configuration, ipmgmt_handler() in usr/src/cmd/cmd-inet/lib/ipmgmt/ipmgmt_door.c frees the caller's credential with ucred_free() immediately after reading the user ID, and frees it a second time on the error path if the authorization check fails. An unprivileged local user who does not hold the solaris.network.interface.config authorization can send such a request, for example IPMGMT_CMD_RESETIF, to the ipmgmt door, causing ipmgmt to abort; repeated requests place the svc:/network/ip-interface-management service into maintenance, preventing IP interface configuration. The early free was introduced in 2014 to support lx-branded zones (OmniOS commit 4c170900) and is not present in upstream illumos-gate. It affects OmniOS r151020 and later, and SmartOS, prior to the fix.	N/A	More Details
CVE-2026-104114	A NULL pointer dereference in the illumos Network Auto-Magic daemon (nwamd) allows a local user to crash the daemon. nwamd_door_switch() in usr/src/cmd/cmd-inet/lib/nwamd/door_if.c writes to the caller's request structure before checking that a request was supplied, and before checking the caller's credentials. Because the nwamd door at /etc/svc/volatile/nwam/nwamd_door is accessible to all local users, an unprivileged user can issue a door_call() with no argument data to crash nwamd; repeated calls place the svc:/network/physical:nwam service into maintenance, stopping automatic network configuration. nwamd runs only when svc:/network/physical:nwam is enabled, which is not the default. The flaw has existed since 2010 (illumos-gate commit 6ba597c5), and affects any illumos distribution prior to illumos-gate commit 0f1064d9.	N/A	More Details
CVE-2026-92531	Operating system command injection vulnerability in the SVN integration component of BugTracker.NET. The application incorporates the value of the field corresponding to the repository into an svn.exe command without properly validating it. An authenticated user with administrator privileges could store manipulated arguments in the database and subsequently cause them to be processed by the revision comparison functionality. A successful exploit could allow the execution of arbitrary commands with the privileges of the account used by the application. To exploit this vulnerability, svn.exe must be installed and capable of being invoked by the service.	N/A	More Details
CVE-2026-104115	A stack-based buffer overflow in the illumos reparse point daemon (reparse) allows a local user to crash the daemon. get_fs_locations() in usr/src/cmd/fs.d/nfs/rp_basic/libnfs_basic.c, part of the nfs-basic reparse plugin, copies the host and path components of a reparse string into a fixed 1024-byte stack buffer without checking their length. The reparsed door at /var/run/reparsed_door is readable by all users and the door server does not check the caller's credentials, so an unprivileged local user can send an nfs-basic request with an overlong host or path component to overflow the buffer. On systems built with stack protection, which is the default, this causes reparsed to abort; repeated requests place the svc:/system/filesystem/reparse service into maintenance. The service is disabled by default. The flaw has existed since 2009 (illumos-gate commit 2f172c55), and affects any illumos distribution prior to illumos-gate commit 6a2df4aa.	N/A	More Details
CVE-2026-104116	A missing authorization check in the illumos zones statistics daemon (zonestatd) allows a local user in any zone to disrupt zonestat in other zones and to determine which zones are running. The zonestatd door server procedure, zsd_server() in usr/src/cmd/zonestat/zonestatd/zonestatd.c, handles the ZSD_CMD_NEW_ZONE command, which is intended to be sent by zoneadmd, without checking the caller's credentials. Because the zonestatd door is accessible to all users in every zone, an unprivileged user can send this command with an arbitrary zone ID, causing zonestatd to re-create its door file in that zone, so that new zonestat requests in that zone can fail while the file is replaced. The time taken to handle the command also reveals whether a given zone ID belongs to a running zone. The flaw has existed since 2010 (illumos-gate commit efd4c9b6), and affects any illumos distribution prior to illumos-gate commit 865b58d2.	N/A	More Details
CVE-2026-104117	A missing authorization check in the illumos IP management daemon (ipmgmt) allows a local user to change the persistent IP multipathing (IPMP) configuration. The ipmgmt door dispatch table in usr/src/cmd/cmd-inet/lib/ipmgmt/ipmgmt_door.c does not require the solaris.network.interface.config authorization for the IPMGMT_CMD_IPMP_UPDATE command, although its handler, ipmgmt_ipmp_update_handler(), writes to the persistent ipadm configuration when the IPMGMT_PERSIST flag is set. An unprivileged local user can therefore add interfaces to, or remove them from, existing IPMP groups in the stored configuration. The running configuration is not changed; the modification takes effect when the stored configuration is next applied,	N/A	More Details

	such as at boot, and may disrupt network connectivity. The flaw has existed since 2021 (illumos-gate commit a73be61a), and affects any illumos distribution prior to illumos-gate commit e8d3efa1.		
CVE-2026-105405	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-107806	Nginx UI is a web user interface for the Nginx web server. From 2.3.8 until 2.5.0, an authenticated administrator with an active secure session can submit attacker-controlled portable backup key material and a matching manifest to POST /api/restore. The restore flow trusts the supplied key, decrypts attacker-controlled contents, and replaces the live app.ini, including protected nginx command settings such as TestConfigCmd. Triggering POST /api/nginx/test then executes the restored command in the Nginx UI runtime context, affecting confidentiality, integrity, and availability. This issue is fixed in version 2.5.0.	N/A	More Details
CVE-2026-105404	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-107761	Several Postiz endpoints return the complete database row of the record they operate on instead of only the fields the client needs. Two of them include secrets the caller is not meant to receive. The public API's channel delete returns the deleted integration row, including the channel's platform access token and refresh token. A third-party OAuth app permitted to delete a channel therefore receives that channel's social platform credentials and can use them against the connected account directly, outside Postiz. `GET /user/organizations` returns each organization row, including its API key, to every member of the organization. The API key is intended for admins only, so a member with a lower role can obtain it and call the public API on behalf of the organization. Both endpoints require a valid session, API key or OAuth token and are scoped to the caller's own organization. There is no anonymous access and no cross-tenant exposure.	N/A	More Details
CVE-2026-92393	Apache YuniKorn 1.9.0 and earlier does not implement label and user annotation checks for workload UPDATE action bypassing all checks. Workloads in YuniKorn are defined as the following Kubernetes objects: "deployments", "replicasets", "statefulsets", "daemonsets", "jobs", "cronjobs". The CREATE action correctly enforces the checks for all object types. The bypass allows any user to specify an arbitrary user info annotation. The same bypass also allows changing the application ID for the workload. The combination of the two applied in one UPDATE could allow access to a queue that the user normally would not have access to. Quota usage for the queue might be impacted if the application runs in the incorrect queue. User based quota enforcement is also based on the user annotation. User quota tracking could be side stepped even if the application runs in the correct queue. Users are recommended to upgrade to version 1.10.0, which fixes this issue.	N/A	More Details
CVE-2026-78243	Apache YuniKorn 1.8.0 and later, if configured with the LDAP group resolver, crashes due to an out of bounds read processing group membership entries.If the LDAP server returns a group membership entry, memberOf attribute, for a user specified in the pod the server crashes if a membership record does not start with "CN=". This only affects install that have the non default LDAP group provider configured. Users are recommended to upgrade to version 1.10.0, which fixes this issue.	N/A	More Details
CVE-2026-97715	CVE-2026-97715 is a vulnerability in the client registration process of Secure Access servers prior to version 14.60. Authenticated attackers can pass malformed data to the server and cause a persistent denial of service.	N/A	More Details
CVE-2026-97468	Apache CXF's STSTokenValidator and Security Token Service (STS) cached validated security tokens under a non-cryptographic 32-bit hash of the token (Java Arrays.hashCode/hashCode()), and treated a cache hit as proof that the presented token had already been validated. An attacker could craft a token (for example a UsernameToken or a self-signed SAML Assertion) whose hash collides with a cached entry. The token would then be accepted without password validation, signature trust verification or a call to the STS. This could let the attacker authenticate as another user and, through STS token validation or renewal, obtain STS-signed tokens for that identity. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-97791	In Apache CXF, STSTokenValidator checks whether a SAML assertion is signed by a trusted certificate before deciding to send it to the STS. That result was stored in one object shared by all requests, so one request could read another's result. A remote, unauthenticated attacker could send a forged assertion signed with an untrusted certificate while legitimate requests were being processed, and it could be accepted as trusted without ever reaching the STS. Only services that use STSTokenValidator to validate SAML tokens without alwaysValidateToSts set are affected. Users are recommended to upgrade to versions 4.2.4 or 4.1.9 or 3.6.13, which fix this issue.	N/A	More Details
CVE-2026-107355	Rejected reason: ** This candidate has been removed by an organization.	N/A	More Details
CVE-			

CVE-2026-95125	libming through 0.4.8 contains a heap buffer overflow in r_readc() in src/blocks/fromswf.c. A crafted SWF file with a malformed or truncated RECT header can cause a denial of service.	N/A	More Details
CVE-2026-34499	Use of hard-coded cryptographic key vulnerability in Johnson Controls ADVMS allows Read Sensitive Constants Within an Executable. This issue affects ADVMS: before 3.10.	N/A	More Details
CVE-2026-104703	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-97714	CVE-2026-97714 is a vulnerability in the authentication sub-system of Secure Access servers prior to version 14.60. Attackers can send a malformed response during authentication and cause a persistent denial of service.	N/A	More Details
CVE-2026-105877	Insertion of Sensitive Information Into Sent Data vulnerability in QuarkA QA Analytics qa-heatmap-analytics allows Retrieve Embedded Sensitive Data.This issue affects QA Analytics: from n/a through 5.3.0.0.	N/A	More Details
CVE-2026-105827	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-8374	Misuse and misconfiguration in Bluetooth communication in SwitchBot Door Lock Series allows an attacker to bypass the electronic lock and access controls via a manipulated communication protocol.	N/A	More Details
CVE-2026-97716	CVE-2026-97716 is a vulnerability in the connection set up sub-system of Secure Access servers prior to version 14.60. Unauthenticated attackers can send specially crafted traffic to the server and cause a persistent denial of service.	N/A	More Details
CVE-2026-97717	CVE-2026-97717 is a vulnerability in the proxy sub-system of Secure Access servers prior to 14.60. Authenticated attackers can send malformed data to the server and cause a persistent denial of service.	N/A	More Details
CVE-2026-107363	In OpenStack Zaqr before 23.0.1, the WebSocket transport fails to bind the project identifier in subsequent requests to the project authenticated by the Keystone token. An authenticated user with a valid token for one project may substitute another project's UUID to enumerate, inspect, create, or delete queues belonging to that project, resulting in unauthorized disclosure, modification, or loss of queue data. Only deployments using the WebSocket transport with Keystone authentication are affected.	N/A	More Details
CVE-2026-106581	Before 4.92.0, Docker Desktop for Windows did not verify the signature of a package supplied to Docker Desktop Installer.exe install -package. An attacker able to provide a crafted package and convince a user to approve the Docker-signed UAC prompt could execute attacker-controlled installer actions as LocalSystem.	N/A	More Details
CVE-2026-107785	Crux Agent from 1.9.0 before 2.0.3 uses the full SKA bilocation key as the WireGuard preshared key. When a peering session negotiates use of SHA-512, the key produced is 64 bytes instead of the 32 bytes WireGuard requires. The agent does not validate this size; instead it attempts to use the `wg set` command to update the live tunnel, and write the invalid key to the WireGuard configuration file. The update fails, so the live tunnel keeps using its previous preshared key until the tunnel is shut down. The tunnel will fail to start when restarted. For a peer which has never successfully negotiated a 32-byte bilocation key in a Crux C2 organization which has the "Enforce SKA Use" setting turned off, no preshared key will be set for the tunnel. Therefore, an attacker who is able to intercept and store the peer's traffic, and has access (or will have access) to a cryptographically relevant quantum computer, will be able to decrypt the tunnel.	N/A	More Details
CVE-2026-105828	Parse Server 8.2.2 before 8.6.92 and 9.0.0 before 9.10.1-alpha.12 contains an information disclosure vulnerability in which GraphQL validation error messages reveal hidden class names when public introspection is disabled. Unauthenticated attackers holding only the public Application Id can send crafted operations triggering unknown-argument or invalid enum value errors to learn pointer and relation target classes.	N/A	More Details
CVE-2026-105403	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-105402	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-105401	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details

CVE-2026-108266	Privasys rustls is a maintained fork of the rustls TLS library that adds RA-TLS challenge and channel-binding support. Prior to privasys-v0.8.1, the fork emitted RA-TLS challenge certificates whose quote ReportData was bound to the certificate public key and client nonce but not to the active TLS session. An attacker who obtained an enclave TLS private key could relay a genuine quote onto another connection, causing a relying party to accept an attacker-terminated connection as the attested enclave. This issue is fixed in privasys-v0.8.1.	N/A	More Details
CVE-2026-104758	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-73364. Reason: This candidate is a reservation duplicate of CVE-2026-73364. Notes: All CVE users should reference CVE-2026-73364 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-78797	An issue in iStoreOS istoreos-24.10.7 and before allows a remote attacker to execute arbitrary code via the task_id in tasks-lib.lua.	N/A	More Details
CVE-2026-107852	Jexactyl is a customisable game management panel and billing system. Prior to 4.0.5, the POST /api/client/billing/stripe/process endpoint accepts a client-supplied Stripe Checkout Session when payment_status is paid but does not compare amount_total or currency with the referenced order and configured billing currency. On an instance where the billing module is enabled and a Stripe secret key is configured, an authenticated client can therefore complete a lower-value or mismatched-currency payment and cause the order to be processed, provisioning, renewing, upgrading, or unsuspending the purchased server for less than the required price. This issue is fixed in version 4.0.5.	N/A	More Details
CVE-2026-107175	MISP contains a defect in its event save workflow that prevents the correlation engine from recalculating correlations when an event's distribution level or sharing group is modified. When a user edits an existing event and changes its distribution or sharing_group_id, the internal before-save hook stored the incoming (new) data rather than the previously persisted values. As a result, the after-save comparison that determines whether a correlation refresh is needed never detected the change, and stale correlations persisted. Security impact: - Stale correlations may continue to expose event data to users in a broader sharing group after the event has been moved to a more restrictive group, resulting in unintended information disclosure. - Conversely, newly relevant correlations may not appear after a distribution widening, degrading the completeness of threat intelligence sharing. Preconditions: - An authenticated user with write access to at least one MISP event. - The user modifies the event's distribution or sharing_group_id field. Affected versions: <2.5.48	N/A	More Details
CVE-2026-108258	Shiny for Python is a framework for building interactive web applications in Python. From 1.4.0 until 1.6.4, bookmark restore accepts a client-supplied state_id and joins it into the server-side shiny_bookmarks directory without validating that it is a single safe path segment. An unauthenticated request can use parent-directory segments or an absolute path to make the server open input.json and values.json outside the bookmark store, even when bookmark_store is set to disable. In applications configured with bookmark_store set to server and using ui.input_file(), the restore handler can additionally copy and expose an attacker-selected file from an attacker-selected directory. This issue is fixed in version 1.6.4.	N/A	More Details
CVE-2026-107180	On MISP instances configured to require TOTP enrolment (Security.otp_required), the enforcement of the mandatory two-factor authentication setup applied only to standard browser requests. An authenticated user who had not yet enrolled in TOTP could bypass the forced setup by issuing any non-browser request type, including AJAX/XHR calls, REST API requests, .json format URLs, restSearch queries, or automation actions. Because these machine-readable request shapes cannot follow the redirect that the browser path uses to send the user to the TOTP enrolment page, the guard simply skipped the check and the user retained full access to the instance without completing the required second-factor setup. The initial fix (commit 8deb0619e) added a guard specifically for AJAX requests. A follow-up fix (commit 6b527ba6e) broadened the guard to cover every non-browser request shape, while preserving the exemption for identities authenticated via API key (logged_by_authkey flag). Impact: an authenticated user on an otp_required instance can operate with full access indefinitely without enrolling in TOTP, nullifying the instance-level two-factor authentication policy. Affected version: <2.5.48	N/A	More Details
CVE-2026-108265	Enclave OS Mini is a Rust-based runtime for confidential applications inside Intel SGX enclaves. Prior to wasm-v0.40.0, the SGX runtime's RA-TLS challenge certificate path placed the certificate public-key hash and client nonce in quote ReportData but omitted a value bound to the active TLS session. An attacker who obtained an enclave TLS private key could relay a genuine quote onto another connection, causing a relying party to accept an attacker-terminated connection as the attested enclave. This issue is fixed in wasm-v0.40.0.	N/A	More Details
CVE-2026-62367	Vikunja is an open-source self-hosted task management platform. In versions 1.0.0 through 2.3.0, when an administrator enables the per-provider `emailfallback` option on an OpenID Connect provider, Vikunja links an SSO login to a pre-existing local (username+password) account using only the `email` claim from the IdP. The fallback never checks an `email_verified` (or Microsoft `xms_edov`) signal and never requires the matched account's password. An attacker who can obtain a token from the configured issuer carrying a victim's email logs in as that victim with a full session, with no consent or interaction from the victim. Version 2.4.0 fixes the issue.	N/A	More Details

CVE-2026-75353	OpENer v2.3/ commit 76b95cf, contains an out-of-bounds read in the server-side EtherNet/IP ForwardOpen connection-path parser. This allows a remotoe attacker to cause a denial of service	N/A	More Details
CVE-2026-108267	Privasys Go is a maintained fork of the Go programming language that adds RA-TLS support to crypto/tls. Prior to privasys-v0.5.1-go1.26.5, challenge-mode RA-TLS certificates bound quote ReportData to the certificate public key and client nonce but not to the active TLS session. An attacker who obtained an enclave TLS private key could relay a genuine quote onto another connection, causing a relying party to accept a handshake terminated by the attacker as an attested enclave connection. This issue is fixed in privasys-v0.5.1-go1.26.5.	N/A	More Details
CVE-2026-108268	Enclave OS Virtual runs container workloads inside confidential virtual machines with end-to-end attestation. Prior to tdx-v0.2.43 and tdx-gpu-v0.6.27, the TDX/GPU RA-TLS certificate issuer placed the certificate public-key hash and client nonce in quote ReportData but omitted a value bound to the active TLS session. An attacker who obtained an enclave TLS private key could relay a genuine quote onto another connection, causing a relying party to accept an attacker-terminated connection as the attested enclave. This issue is fixed in tdx-v0.2.43 and tdx-gpu-v0.6.27.	N/A	More Details
CVE-2026-108269	Remote Attestation TLS Clients provides multi-language utilities for verifying attested TLS connections. Prior to 0.5.0, the Rust and Go RA-TLS challenge verifiers accepted quote ReportData that was bound to the certificate public key and client nonce but not to the active TLS session before permitting application traffic. An attacker who obtained an enclave TLS private key could relay a genuine quote onto another connection, causing the clients to accept an attacker-terminated connection as the attested enclave. This issue is fixed in 0.5.0.	N/A	More Details
CVE-2026-103755	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-16681	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-18524	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-22061	Trident versions v25.02.1 through v26.06.1 are susceptible to a vulnerability that could allow an authenticated attacker with access to debug logs to view LUKS passphrases or SMB Active Directory credentials.	N/A	More Details
CVE-2025-8457	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-102783	Joomla Extension - balbooa.com - Path Traversal in image preview Gridbox < 2.20.4.0 - Gridbox contains the same prefix-only containment logic in its site UploaderHelper . The showImage action resolves a request-controlled path, calls that helper, and then returns the image. If image decoding is unavailable or fails, the action streams the file directly. An existing image in a sibling directory such as images-backup can therefore satisfy the current containment test even though it is outside the configured images root. The route restricts the file extension to Gridbox image types, which materially limits the read primitive. The default media root is images ; the effective site setting was not independently verified. No prefix-matching sibling directory was found alongside the site's images directory. The finding is rated Low rather than presented as arbitrary file disclosure.	N/A	More Details
CVE-2026-108125	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in wp-post-author. This issue affects wp-post-author version 4.0.0 prior to 4.1.0.	N/A	More Details
CVE-2026-104634	Incorrect Type Conversion or Cast vulnerability in BeamMCP.Server in ScriptKittyOS beam_mcp allows an MCP client's JSON true, false and null tool arguments to reach the host's dispatch function as the strings "true", "false" and "nil". After BeamMCP.Schema.validate/2 accepted a value as a boolean, normalize_arguments/2 passed every argument through to_json_value/1, whose atom clause converts true, false and nil to strings. A string is truthy in Elixir, so a host that tests a boolean argument, for example if args.dry_run, takes the opposite branch for false, and a guard such as confirm: false reads as set. The client controls the argument and could send true directly, so the practical impact is limited to hosts whose behaviour on false differs from their behaviour on true, and to any policy layer in front of the server that permits false but refuses true. The same normalisation applies to prompts/get arguments, which exist from 0.5.0. This issue affects beam_mcp: from 0.1.0 before 0.10.1.	N/A	More Details
CVE-			More

2026-105400	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	Details
CVE-2026-105399	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-105398	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Details
CVE-2026-105331	Local privilege escalation in Checkmk 2.5.0 before 2.5.0p10 allows a user with access to edit the Oracle Instant Client referenced by the agent plugin 'mk-oracle' to escalate their privileges if an agent has this plugin enabled.	N/A	More Details
CVE-2026-78796	An issue in Netcore B11 Enterprise-level full Gigabit 9-port shop wireless router v1.3.241114.024540 and before allows a remote attacker to execute arbitrary code via the www/cgi-bin/upgrade file	N/A	More Details
CVE-2026-95702	Use-after-free vulnerability in VFS in Google gVisor prior to release 20260831.0 on all platforms allows a local attacker with standard container privileges to achieve code execution in the host sentry process by double-freeing the backing MemoryFile from an in-sandbox overlay filesystem. The sentry process remains confined by host-level Linux seccomp and namespace boundaries.	N/A	More Details
CVE-2026-102554	Allocation of resources without limits or throttling (CWE-770) during Java object deserialization in Google Guava versions 4.0 through 33.7.1 allows an attacker to cause a Denial of Service via OutOfMemoryError. When deserializing CompactHashMap, CompactHashSet, or MapMakerInternalMap instances, Guava eagerly allocates an array based on a caller-specified size parameter without throttling, permitting memory exhaustion from crafted serialization streams.	N/A	More Details
CVE-2026-92532	Unrestricted file upload vulnerability in the BugTracker.NET attachment functionality. An authenticated user with administrator privileges could modify the application configuration to store files in a directory accessible via the web interface. Due to the lack of proper file extension validation, an attacker could upload a malicious ASPX file and subsequently execute it on the server. A successful exploit could allow arbitrary code execution with the privileges of the account used by the web service.	N/A	More Details
CVE-2026-102784	Joomla Extension - balbooa.com - CSRF in language installation feature Gridbox < 2.20.4.0 - PagesController uses a trait that validates the Joomla session token only when the HTTP method is POST. addLanguage does not require POST inside the action and reads url and zip through the generic request input. A GET request can therefore reach the action without the trait checking a token. The action still requires core.tools , but that is the victim's permission check; it does not prove that the privileged user intended the request.	N/A	More Details
CVE-2026-92533	Path traversal vulnerability in the BugTracker.NET file download component. The parameter used to specify the file name does not properly validate user-supplied paths. An authenticated remote attacker could enter a manipulated path to access files located outside the intended directory. Successful exploitation could allow the attacker to read system files accessible to the account used by the application.	N/A	More Details
CVE-2026-103663	Ollama is vulnerable to path traversal in the `/api/pull` endpoint due to insufficient validation of layer digests by the `digestToPath` function. An unauthenticated remote attacker can specify a path traversal sequence as a layer digest, causing a malicious binary to be written outside the model store. Critically if the server process has write access to `/usr/lib/ollama` (the default in most Ollama Docker images), an attacker can write the malicious file to that directory. On the next server restart, the file is loaded and executed, resulting in remote code execution as root. This issue was fixed in version 0.35.0.	N/A	More Details
CVE-2026-96408	A code injection vulnerability exists in the upgrade script of Movable Type, which may allow an unauthenticated attacker to execute an arbitrary Perl script or an SQL query on the affected product.	N/A	More Details
CVE-2025-61560	A race condition vulnerability in the SessionManager of CNCF: Cloud Native Computing Foundation Argo CD v3.0.6 allows attackers to bypass rate limiting and perform a brute force attack via repeated crafted requests.	N/A	More Details
CVE-2026-107824	x64dbg-MCP Server is a native Model Context Protocol (MCP) plugin for x64dbg that exposes the debugger's full functionality over HTTP. Prior to 1.1, x64dbg-MCP Server exposes all MCP debugger tools over HTTP and SSE without authentication while listening on 0.0.0.0 by default. Any unauthenticated network client that can reach the default port, 9094 for x64 or 9095 for x32, can execute arbitrary x64dbg commands, attach to processes by PID, read and write debuggee memory, and write files to arbitrary paths. This issue is fixed in version 1.1.	N/A	More Details
CVE-	Claude Code validated that a target file path resided within the project working directory at permission-check time, but re-resolved the path at write time without repeating that validation. This time-of-check to time-of-use (TOCTOU) gap allowed an attacker who could write to the workspace to atomically replace a project file with a symlink, causing Claude Code to follow the symlink and write its output to an arbitrary file outside the		

2026-103435	project sandbox. Exploitation required the ability to win a race condition against the write operation and write access to the shared workspace, enabling a lower-privileged attacker to redirect benign edits to sensitive files (e.g., shell configuration) in a higher-privileged session. Users on standard Claude Code auto-update have received this fix already. Users performing manual updates are advised to update to the latest version. Thank you to hackerone.com/c_h4ck_0 for reporting this issue.	N/A	More Details
CVE-2026-107836	RIOT is an open-source microcontroller operating system designed for Internet of Things devices and other embedded systems. In 2026.07 and earlier, the nanoCoAP client function nanocoap_sock_get_slice() in sys/net/application_layer/nanocoap/sock.c accepts a Block2 response when _block_cb() sees the expected block number without also verifying that the server-controlled szx and derived offset match the requested block geometry. A malicious CoAP server can return the expected block number with a larger block size, causing the derived offset to exceed the client slice offset and making ctx->offset - offset underflow in _2buf_slice(). The resulting buffer-relative calculation can read before the payload buffer and crash the client, causing denial of service and potentially exposing adjacent memory. No fixed release is available as of this review.	N/A	More Details
CVE-2026-88257	Improper Input Validation vulnerability in BeamMCP.Schema in ScriptKittyOS beam_mcp allows an MCP client to reach a tool's dispatch function with arguments that violate the input schema the server advertised. BeamMCP.Schema.validate/2 checked type, required, additionalProperties, enum and numeric bounds on the top-level arguments object only. Constraints inside nested objects and on array items (items, minItems, maxItems, minLength, maxLength, pattern, nested required, enum and additionalProperties: false) were advertised by tools/list and never checked at tools/call or prompts/get, and keywords outside the enforced subset (oneOf, anyOf, \$ref) were advertised and ignored. A host whose dispatch code relies on the schema it declared receives values the schema forbids, such as an out-of-range number or an undeclared key inside a nested object. What the host does with such a value decides the impact. This issue affects beam_mcp: from 0.1.0 before 0.10.1.	N/A	More Details