SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 November 2026

Generated on 18 November 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-2026-124815	The Clockinator Lite WordPress plugin before 1.1.0 does not restrict access to several of its record deletion actions, and uses a user-supplied table name in a SQL query without validating or escaping it, allowing unauthenticated users to perform SQL injection attacks, deleting data from any database table and extracting sensitive information such as password hashes.	10.0	More Details
CVE-2026-129444	A vulnerability was identified in D-Link DSL-6740C 20131126. This affects an unknown function of the file /etc/templates/ftpd/ftpd_conf.php of the component FTP Daemon. Such manipulation leads to hard-coded credentials. The attack can be executed remotely. The exploit is publicly available and might be used.	10.0	More Details
CVE-2026-124822	The Easy DragDrop File Uploader WordPress plugin before 1.1.10 does not validate a user-supplied path before deleting it, allowing unauthenticated users to delete arbitrary files and directories on the server, such as wp-config.php.	10.0	More Details
CVE-2026-127275	A vulnerability was determined in Linksys EA8100 1.0.3.216940. This issue affects the function SetRemoteSetting/SetUnsecuredWiFiWarning of the file ui_server.lua of the component JNAP API. This manipulation of the argument isEnabled/enabled causes missing authentication. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-129351	A security vulnerability has been detected in TRENDnet TEW-657BRM 1.00.1. This vulnerability affects the function sprintf of the file /setup.cgi of the component mini_httpd. Such manipulation leads to out-of-bounds write. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor explains: ""I am not able to confirm if such vulnerability exists as the product has been EOL for more than 15 years. We will send out an announcement letting customers know." This vulnerability only affects products that are no longer supported by the maintainer.	10.0	More Details
CVE-2026-129353	A vulnerability was detected in D-Link DIR-600L 2.17/2.17b02. Affected by this vulnerability is the function authenticationcgi_main of the file authentication.cgi. Performing a manipulation of the argument id/password results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.	10.0	More Details
CVE-2026-129354	A flaw has been found in D-Link DIR-600L 2.17b02. Affected by this issue is the function hnap_main of the file htdocs/cgibin of the component HNAP Handler. Executing a manipulation can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	10.0	More Details
CVE-2026-78287	Improper Control of Generation of Code ('Code Injection') vulnerability in Staggs STAGGS staggs allows Remote Code Inclusion.This issue affects STAGGS: from n/a through 3.3.0.	10.0	More Details

CVE-2026-127277	A security flaw has been discovered in Linksys EA8100 1.0.3.216940. The affected element is an unknown function of the file etc/init.d/service_smbd.sh of the component SMB Service. Performing a manipulation of the argument ANON_ACCESS results in improper initialization. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-127073	OpsTree BuildPiper before 2.7.0 contains a privilege escalation vulnerability that allows project users to gain Kubernetes cluster-admin rights by submitting unrestricted manifests through the Additional Manifest feature. Attackers can deploy a ClusterRoleBinding binding a service account to cluster-admin, which the pipeline applies with cluster-wide credentials, granting control over all workloads and secrets.	9.9	More Details
CVE-2026-125851	Unrestricted Upload of File with Dangerous Type vulnerability in themagnifico52 Hotel Booking Lite hotel-booking-lite allows Upload a Web Shell to a Web Server.This issue affects Hotel Booking Lite: from n/a through 2.5.1.	9.9	More Details
CVE-2026-129450	A vulnerability was detected in DrayTek Vigor2960 1.5.1.6. Affected by this issue is the function sub_1E084 of the file /cgi-bin/mainfunction.cgi?action=doWebBackup. The manipulation of the argument option results in path traversal. It is possible to launch the attack remotely. The exploit is now public and may be used. Upgrading to version 1.5.1.7 can resolve this issue. You should upgrade the affected component. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	9.9	More Details
CVE-2026-129451	A flaw has been found in DrayTek Vigor2960 up to 1.5.1.6. This affects the function app_guest_export of the file /cgi-bin/mainfunction.cgi. This manipulation of the argument filename causes path traversal. The attack can be initiated remotely. The exploit has been published and may be used. Upgrading to version 1.5.1.7 is able to mitigate this issue. The affected component should be upgraded. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	9.9	More Details
CVE-2026-12591	Zohocorp ManageEngine M365 Manager Plus versions below 4818 is affected by an authenticated technician may exploit insufficient permission validation in the delegated administration interface to escalate privileges beyond their intended scope, which could result in remote code execution during administrative processing.	9.9	More Details
CVE-2026-127080	OpsTree BuildPiper before 2.7.0 contains an improper authorization vulnerability that allows authenticated deploy users to define arbitrary Kubernetes hostPath volumes without allow-list or policy checks. Attackers can set the host path to / in the Define HostPath Volume configuration to mount the worker node root filesystem read-write, breaking container isolation and enabling node and cluster compromise.	9.9	More Details
CVE-2026-110697	A flaw was found in Quay where the robot account listing function constructs a SQL LIKE pattern from user-controlled namespace names without escaping wildcard metacharacters. An attacker who creates a namespace containing an underscore character can match and retrieve robot accounts and their decrypted authentication tokens from other tenants' namespaces, leading to cross-tenant credential theft and unauthorized image operations.	9.9	More Details
CVE-2026-129433	Dokploy before 0.31.1 contains an OS command injection vulnerability in getComposeContainerCommand() that allows authenticated organization members to execute shell commands via the serviceName parameter. Attackers can store serviceName values with shell metacharacters through backup.create or backup.update tRPC procedures, executing commands as root when scheduled backups run and taking over the host via the mounted Docker socket.	9.9	More Details
CVE-2026-129449	A security vulnerability has been detected in DrayTek Vigor2960 up to 1.5.1.6. Affected by this vulnerability is the function sub_14914 of the file /cgi-bin/mainfunction.cgi. The manipulation of the argument swmconfigupload leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.5.1.7 addresses this issue. It is advisable to upgrade the affected component. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	9.9	More Details
CVE-2026-129250	A security vulnerability has been detected in Edimax BR6478ACV2 1.23. The impacted element is the function formPPTPSetup of the file webs. The manipulation of the argument pptpUserName leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.9	More Details
CVE-2026-129453	A vulnerability was found in DrayTek Vigor2960 1.5.1.6. This issue affects the function check_file_exist of the file /cgi-bin/mainfunction.cgi of the component File Existence Check. Performing a manipulation of the argument upload_name results in heap-based buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used. Upgrading to version 1.5.1.7 is capable of addressing this issue. Upgrading the affected component is recommended. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	9.9	More Details
CVE-2026-	A prompt injection vulnerability in all versions of Jet Admin Cloud Platform allows a remote attacker with a		More

123965	free account to expose sensitive .env configuration files and exfiltrate critical credentials. Mitigated via sandbox component around October 29, 2026.	9.9	Details
CVE-2026-126119	The Streamit WordPress plugin before 1.3.10 does not perform any authorization or nonce verification on one of its unauthenticated AJAX routes, which invokes an attacker-supplied PHP function with an attacker-supplied argument array, allowing unauthenticated attackers to call arbitrary functions (for example to create an administrator account), leading to privilege escalation and remote code execution.	9.8	More Details
CVE-2026-126315	Frappe HRMS 16.14.0 before 16.20.1 sends product usage events on certain HR transactions without checking the site's telemetry setting, and some events include more detail than needed. During normal use, with no user action, values such as leave type names, claimed amounts and appraisal scores are transmitted even when telemetry is disabled.	9.8	More Details
CVE-2026-125055	The Chatterbug Forms – Fast, Flexible WordPress Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.0.2 via the cbforms_check_form_submissions function. This is due to missing server-side file extension validation in cbforms_check_form_submissions(), where the allowed-type check defaults to the uploaded file's own extension when no field restriction is configured, trivially allowing any extension including .php. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The submission nonce printed inline on every public page containing a Chatterbug form is freely obtainable by unauthenticated visitors and therefore does not constitute an effective access control barrier.	9.8	More Details
CVE-2026-119077	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.3.9 via the 'form (specifically the attacker-controlled ticket_label field inside the url-encoded form string)' parameter parameter. This is due to missing server-side authentication and the absence of a class allowlist on deserialization, with the only guard being a nonce publicly emitted on any page carrying the [wsdesk_support] shortcode. This makes it possible for unauthenticated attackers to execute code on the server. A successful exploit requires a single anonymous GET to any public page carrying the [wsdesk_support] shortcode to harvest the publicly emitted wsdesk_nonce value, after which a single unauthenticated POST completes the attack.	9.8	More Details
CVE-2026-124004	XWEB EVO before 5.6.2 contains a hardcoded backdoor password vulnerability that allows unauthenticated remote attackers to gain full administrative access to the built-in Administrator account. Attackers can authenticate using the hardcoded credential xwebevonewgeneration in a single request to obtain a complete admin session and full control over the application. This product line reached it's end of service date in March 2026.	9.8	More Details
CVE-2026-124833	The Ahime Image Printer WordPress plugin through 1.0.0 does not validate the name, extension or type of uploaded files before writing them to disk, allowing unauthenticated attackers to upload arbitrary files, including PHP, and execute code on the server.	9.8	More Details
CVE-2026-118064	The Advance Guest Post WordPress plugin through 1.9 does not properly restrict or validate file uploads, authorizing an upload action with a nonce exposed to every front-end visitor and checking only a file's leading bytes, allowing unauthenticated users to upload arbitrary PHP files and execute code remotely. Successful exploitation additionally requires the target to run PHP 7.x; on PHP 8.0 and later the vulnerable code path raises a fatal error before the file is written.	9.8	More Details
CVE-2026-74911	Software installed and run as a non-privileged user may conduct improper GPU system calls to the execution of an error path that triggers an OOB read & write. An error can be triggered which causes the index of the array element to be cleaned up by the error path would be outside of the array bounds.	9.8	More Details
CVE-2026-124002	XWEB EVO versions 5.2.3 through before 5.7.0 contains a pre-authentication OS command injection vulnerability that allows unauthenticated remote attackers to execute arbitrary OS commands by injecting shell metacharacters into the username field of login.lua, cleanout.lua, or api.lua before the password check occurs. Attackers can exploit this flaw combined with the setuid-root wlua interpreter to execute commands with root privileges, achieving full system compromise. This product line reached it's end of service date in March 2026.	9.8	More Details
CVE-2026-124010	XWEB EVO before 5.6.2 contains a command injection vulnerability that allows unauthenticated remote attackers to execute arbitrary commands as root by exploiting the setuid-root CGI xwconsole.cgi. Attackers can supply malicious input through the sh parameter, which is passed unsanitized to popen(), to achieve full system compromise. This product line reached it's end of service date in March 2026.	9.8	More Details
CVE-2026-118063	The Advance Guest Post WordPress plugin through 1.9 does not properly validate uploaded files, relying on a case-sensitive and incomplete extension check that unauthenticated users can trivially bypass, allowing them to upload arbitrary files, including executable PHP variants, into a web-reachable directory, which can lead to remote code execution depending on the server configuration.	9.8	More Details
CVE-2026-126542	WWBN AVideo 6.5 through 29.7.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to log in as any user via Hybridauth social login display names. Attackers can set their X, Facebook, Yahoo or LinkedIn display name to a victim's username and withhold email, causing login.json.php or oauth2.php to log them in as that account, including administrators, without a password.	9.8	More Details
	FrankenPHP Docker images before 1.1.11 were rebuilt only when new base image tags were created, so		

CVE-2026-128027	security fixes that Alpine, PHP, and Go applied under existing tags were not propagated. Remote attackers could exploit known flaws in the stale system libraries, such as CVE-2025-15467 in libcrypto3, to execute code.	9.8	More Details
CVE-2026-109445	PLANET GS-5220-8P2T2S (hardware version 3.0) firmware versions before 3.2412b261008 contains a stack-based buffer overflow vulnerability that allows unauthenticated attackers to corrupt stack memory by submitting an oversized webstax_auth HTTP Cookie value that is copied into a fixed-size stack buffer without length validation. Attackers can send a crafted unauthenticated HTTP request with an oversized cookie to overwrite the saved return address and corrupt stack memory, leading to memory corruption and potential denial of service on the device.	9.8	More Details
CVE-2026-125769	Incorrect Privilege Assignment vulnerability in Nasir Ahmed Advanced Form Integration advanced-form-integration allows Privilege Escalation.This issue affects Advanced Form Integration: from n/a through 2.11.3.	9.8	More Details
CVE-2026-122662	Deserialization of Untrusted Data vulnerability in Barn2 Plugins Document Library Pro document-library-pro allows Object Injection.This issue affects Document Library Pro: from n/a before 4.2.2.	9.8	More Details
CVE-2026-127048	The Custom Block Builder WordPress plugin before 3.0.0 does not properly deny unauthorised requests to its REST routes, as its permission checks return a non-error response that WordPress treats as granted, allowing unauthenticated users to execute arbitrary PHP code on the server.	9.8	More Details
CVE-2026-110960	The Auth Armor WordPress plugin through 1.0.3 does not require authentication on several handlers available to logged-out users, which leak the site's stored API credentials and allow an unauthenticated attacker to reset an administrator's enrollment and take over that administrator account.	9.8	More Details
CVE-2015-10149	Dancer versions before 1.3400 for Perl pass unvalidated session ids from the session cookie to the session engine. read_session_id returns the cookie value as the session id without checking its characters, and Dancer hands it to the session engine to load the session. A remote attacker may cause path traversal or injection in a session engine that uses the id in a file path, cache command or query without checking it.	9.8	More Details
CVE-2011-10042	HTTP::Session versions before 0.43 for Perl allow memcached command injection via unfiltered session ids in HTTP::Session::Store::Memcached. The session id from the client's cookie reaches memcached unchanged as the cache key. A CR and LF in the session id end the cache command early, and the server reads the bytes after them as further commands.	9.8	More Details
CVE-2026-19907	The Shipo plugin for WordPress is vulnerable to Authentication Bypass in versions 1.6 through 1.8.0. This is due to the `authenticate_rest_user()` function parsing the `LOGGED_IN_COOKIE` value and authenticating the named user without verifying the cookie's cryptographic signature. The function's intended `/wp-json/shipo/` route restriction can also be bypassed by placing that substring in the query string of an unrelated REST endpoint. This makes it possible for unauthenticated attackers who know an existing username to impersonate that user, including an administrator, and perform authorized actions through the REST API, including creating another administrator account.	9.8	More Details
CVE-2026-120522	The Cloud Storage Manager for Fluent Forms – Google Drive, Dropbox, OneDrive, S3 Uploads plugin for WordPress is vulnerable to Arbitrary File Write in all versions up to, and including, 1.2.0. This is due to missing authorization checks on the `connection/{driver}/save` and `/download/single-file` REST endpoints, combined with insufficient path validation in the Google Drive `downloadFile()` function, where the Google Drive metadata `name` value is concatenated into a local path without `basename()`, `sanitize_file_name()`, or canonical path validation. This makes it possible for unauthenticated attackers to store attacker-controlled Google Drive credentials, trigger a download of an attacker-owned file whose provider-returned filename contains path traversal, and write attacker-controlled content outside the intended `downloads` directory. When the written file has a PHP extension and lands in a web-accessible location, this can lead to remote code execution.	9.8	More Details
CVE-2026-129114	JSON::XS versions from 3.04 before 4.05 for Perl write one byte past a heap buffer when appending a one-byte chunk in incr_parse. The incremental buffer grows to one and a half times the length it must hold, with no room reserved for the terminating NUL. For an empty buffer and a one-byte chunk that request is one byte, which a buffer whose front was removed by earlier decodes can already have, so nothing is reallocated and the NUL lands one byte past the allocation. A peer streaming data to an incr_parse consumer, choosing how the input is split into reads, can cause a one-byte heap out-of-bounds write.	9.8	More Details
CVE-2026-126173	The AutomatorWP Pro plugin for WordPress' webhook addon is vulnerable to authorization bypass in all versions up to, and including, 1.4.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to reset the password of any WordPress account, including administrators, resulting in full account takeover. This is only exploitable when an administrator has configured an automation pairing a Receive Webhook trigger — with an 'Is the user ID' field — to an Update-User action whose User ID field is left blank and whose Password field is mapped to the webhook password tag, which is a documented, supported plugin configuration.	9.8	More Details
CVE-2026-82504	VITEC EZ TV Platform Server before 8.5.0 contains an unrestricted file upload vulnerability in the upload handler that allows unauthenticated remote attackers to upload arbitrary files by supplying a target filename in the X-FILENAME request header with no authentication or file type validation required. Attackers can upload a malicious ASPX file directly to the web-accessible uploads directory, where it is	9.8	More Details

	immediately executable by the web server, achieving remote code execution in the context of the web server process. Patches are available for versions 8.3.0, 8.3.1, 8.4.0, and 8.4.1. Users running releases prior to 8.3.0 should upgrade to 8.5.0+.		
CVE-2026-124814	The Ultimate Addons for Elementor Forms WordPress plugin before 1.0.8 does not properly validate the extension of uploaded files in its bundled file upload field, allowing unauthenticated users to upload arbitrary files such as PHP scripts and achieve remote code execution.	9.8	More Details
CVE-2026-63079	RBH Access Technologies Integra32 Security Management System 5.1.11 R5.0 contains an unauthenticated deserialization vulnerability in its deprecated .NET Remoting service, exposed on TCP port 2001 via the AxcvcLt.dll library using BinaryServerFormatterSinkProvider at TypeFilterLevel.Full without requiring authentication. A remote unauthenticated attacker can send a malicious serialized gadget payload (such as a ysoserial.net TypeConfuseDelegate chain) to the IntegraURI object endpoint, or exploit MarshalByRefObject/MarshalByValue unmarshalling for arbitrary file read/write and SMB/NTLMv2 credential coercion, to achieve remote code execution as NT AUTHORITY\SYSTEM and fully compromise the host.	9.8	More Details
CVE-2026-129110	sysPass 3.0.1 through 3.2.11 contains an authentication bypass vulnerability that allows unauthenticated attackers to reinstall an already-installed instance by POSTing to the install/install handler, which never checks isInstalled(). Attackers can overwrite config.xml, point the application at an attacker-controlled database, create an administrator account, and plant serialized PublicLink gadget chains triggered via account/viewLink to execute commands.	9.8	More Details
CVE-2026-125855	Deserialization of Untrusted Data vulnerability in Elextensions ELEX WordPress HelpDesk & Customer Ticketing System elex-helpdesk-customer-support-ticket-system allows Object Injection.This issue affects ELEX WordPress HelpDesk & Customer Ticketing System: from n/a through 3.3.9.	9.8	More Details
CVE-2026-129171	NginxPulse 1.5.0 before 1.6.26 contains an unauthenticated sql injection vulnerability that allows remote attackers to append SQL via the id and locationType parameters of /api/stats/:type. Attackers can close the quoted table-name identifier and use error-based output to read database contents, and read or write server files via PostgreSQL superuser functions.	9.8	More Details
CVE-2026-125795	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Estatik Estatik estatik allows PHP Local File Inclusion.This issue affects Estatik: from n/a through 4.3.6.	9.8	More Details
CVE-2026-110959	The Descope WordPress plugin before 1.2.0 does not validate the authentication token it receives before creating a WordPress session, accepting any non-empty token, so an unauthenticated attacker can obtain a session for any existing account, including an administrator, by supplying that account's email address.	9.8	More Details
CVE-2026-123374	Deserialization of Untrusted Data vulnerability in Apache Roller. When Roller sends a weblog update ping, its XML-RPC client deserializes Java object data contained in the ping target's response, so a party that controls that response can run code in the Roller server process. This issue affects Apache Roller from 4.0 through 6.1.6. Users are recommended to upgrade to version 6.1.7, which removes the unsafe deserialization.	9.8	More Details
CVE-2026-126262	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12 may allow an unauthenticated attacker who has access to the oftp port to execute code or command on the system via crafted OFTP packets.	9.8	More Details
CVE-2026-126259	A missing authentication for critical function vulnerability in Fortinet FortiOS 8.0.0, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13, FortiOS 7.0 all versions may allow an unauthenticated attacker with HA FGSP + standalone-config-sync, or autoscale to execute command as super admin via crafted HA packets.	9.8	More Details
CVE-2026-97040	Building a package containing a crafted ".syso" file could bypass cgo flag validation and inject arbitrary linker flags when linking. When loading ".syso" entries from a package archive, the linker only checked for recognized host object headers (ELF, Mach-O, PE, and XCOFF) before falling through to Go object parsing. A ".syso" file beginning with a "go object" header was parsed as a Go compiler object, allowing untrusted cgo metadata directives (such as "cgo_ldflag" or "cgo_dynamic_linker") embedded in the ".syso" file to be passed to the external linker without validation. Additionally, ".syso" filenames longer than 16 bytes lost their ".syso" extension when truncated in archive headers, and unrecognized ".syso" formats forced external linking in pure-Go builds. The linker now rejects ".syso" files that are not recognized host object formats, and "cmd/go" and "cmd/pack" preserve the ".syso" suffix when truncating long archive member names.	9.8	More Details
CVE-2026-121497	The AskAny WordPress plugin before 2.2.0 does not validate the extension or content of files attached to chat messages, trusting the browser-supplied file type instead, which allows unauthenticated users to upload PHP files and execute arbitrary code when visitor attachments are enabled.	9.8	More Details
CVE-2026-123695	The Security For WooCommerce WordPress plugin through 1.0.16 does not restrict access to several of its REST API routes, allowing unauthenticated users to generate login tokens for every user and then retrieve	9.8	More Details

	them, and so log in as any user, including administrators.		
CVE-2026-126170	A improper encoding or escaping of output vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.2, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer Cloud 8.0.1 through 8.0.2, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer-BigData 7.6.0 through 7.6.2, FortiManager 8.0.0 through 8.0.2, FortiManager 7.6.0 through 7.6.7, FortiManager Cloud 8.0.1 through 8.0.2, FortiManager Cloud 7.6.0 through 7.6.7 may allow an unauthenticated attacker to execute unauthorized code or commands via a specially crafted HTTP request	9.8	More Details
CVE-2026-123710	A flaw was found in Red Hat Quay. An unauthenticated client can obtain an anonymous registry token with an audience it controls, present that token to the service key rotation endpoint, and install its own approved signing key with no expiry. Registry tokens signed with that key are accepted for any repository, allowing read and write access to private images and replacement of repository tags.	9.8	More Details
CVE-2026-67449	Portabase is a database backup and restore tool for PostgreSQL, MySQL, MsSQL, MariaDB, Firebird SQL, SQLite, MongoDB, Redis, Files and Docker Volume. Prior to version 1.21.2, a path traversal in the TUS upload webhook handler (app/api/tus/hooks/route.ts) allowed an unauthenticated attacker to overwrite arbitrary files under the private data directory, including /data/private/keys/master_key.bin (the AES-256-GCM master key). This issue has been patched in version 1.21.2.	9.8	More Details
CVE-2026-126148	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6 may allow an unauthenticated attacker to execute unauthorized code or commands via crafted HA join-request packets.	9.8	More Details
CVE-2026-126147	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.	9.8	More Details
CVE-2026-126812	blueprintUE Self-Hosted Edition before 4.3.7 contains an insecure default configuration in its Docker Compose examples that sets MYSQL_ALLOW_EMPTY_PASSWORD=yes in database.env and publishes MariaDB on port 3306. Unauthenticated attackers reaching the Docker host on port 3306 can log in as root without a password to read, modify, or delete user accounts, blueprints, and all databases.	9.8	More Details
CVE-2026-71395	unsafe deserialization in hyphenation loading vulnerability in Apache XML Graphics FOP. This issue affects Apache XML Graphics FOP: through 2.11. Users are recommended to upgrade to version 2.12, which fixes the issue.	9.8	More Details
CVE-2026-126722	Rooxis RXR-12 Wi-Fi router contains an undocumented telnet backdoor daemon (/usr/bin/telnetd_startup) that, upon receipt of a precomputed AES-128-CBC magic packet using a firmware-wide static key and IV, enables telnet service with default credentials, providing remote root access. Firmware 20260813_c2169ea5 removes the UDP listener entirely, and users can update through their local web interface.	9.8	More Details
CVE-2026-126797	NextScan 1.1.0 through 1.2.0 contains an authentication bypass vulnerability in ns-admin that allows unauthenticated attackers to forge administrator tokens using a hardcoded JWT signing key. Attackers can sign an HS256 X-Access-Token carrying the public super administrator role ID to gain full access to user management, scan tasks and stored vulnerability results.	9.8	More Details
CVE-2026-126263	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.4, FortiMail 7.4.0 through 7.4.6 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	9.8	More Details
CVE-2026-126768	OpsTree REMS through 1.0.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to obtain valid JWTs by setting the client-controlled is_local_auth field. Attackers can send a POST /api/v1/user/login/ request for the admin account with an invalid password and is_local_auth true to gain SuperUser administrative access.	9.8	More Details
CVE-2026-64682	AstroBlocks is a block-first CMS for Astro projects. Prior to version 3.4.0, admin session tokens can be forged due to a hard-coded fallback JWT secret and a mismatched environment variable name. An attacker who knows the public fallback value (readable in the published package) can forge a valid session token with role: "owner" and obtain full administrative control of the CMS — creating/deleting content, users, media, redirects, and configuration. This issue has been patched in version 3.4.0.	9.8	More Details
CVE-2026-76954	An improper neutralization of special elements used in an SQL command vulnerability in the Auth API in Synology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1 allows remote attackers to read or write arbitrary files and conduct denial-of-service attacks.	9.8	More Details
	NOsql Object (NO2 a.k.a Nitrite) database is an open source nosql embedded document store. Prior to version 4.4.1, when Nitrite opens a database file, MVStoreUtils.openOrCreate() automatically checks for a legacy v1-format store and, on detecting one (or hitting a compatibility error while opening), triggers an automatic migration path. This path deserializes stored values using NitriteDataType.deserialize(byte[]), which passes the raw bytes directly to java.io.ObjectInputStream.readObject() via a custom		

CVE-2026-64678	NitriteObjectInputStream subclass. That subclass overrides only readClassDescriptor() — solely to remap a handful of known legacy class names to their current equivalents — and implements no class allowlist, blocklist, or ObjectInputFilter (JEP 290). Any Serializable class reachable on the embedding application's classpath can therefore be instantiated via readObject(), with readObject()/readExternal()/readResolve() callbacks invoked unconditionally. If a suitable gadget class (e.g. from commons-collections or similar) happens to be present on the classpath, this is a precondition for remote code execution. This issue has been patched in version 4.4.1.	9.8	More Details
CVE-2026-126673	Data::Dump::Streamer versions before 3.00 for Perl allow code injection via unescaped Regexp patterns in _dump_qr. A Regexp's pattern is written into a qr literal without escaping "$" or "@", so "@{[...]}" and "${\ ... }" in the pattern run as code when the dump is evaluated. An already escaped delimiter gets a second backslash, which leaves the delimiter bare and ends the qr literal early. An attacker who supplies a pattern that an application compiles, dumps and later restores with eval or do can run arbitrary Perl code.	9.8	More Details
CVE-2026-126909	Use after free in Passwords in Google Chrome prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-126846	Use after free in Skia in Google Chrome on on Android prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-126859	Link following in FileSystem in Google Chrome prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-126254	A numeric truncation error vulnerability in Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13 may allow a configured ibgp neighbor to send malicious/malformed attributes to all connected routers via a specially crafted request	9.6	More Details
CVE-2026-65840	Fider is a feedback portal for feature requests and suggestions. Prior to version 0.36.0, in multi-tenant mode (HOST_MODE=multi), an attacker can use an email verification key issued by Tenant A to authenticate as the same email address on Tenant B. This completely bypasses tenant isolation and allows unauthorized account takeover across tenants. Single-host deployments (HOST_MODE=single, the default) are NOT affected. This issue has been patched in version 0.36.0.	9.6	More Details
CVE-2026-115734	The Pay with a tweet WordPress plugin through 1.0.5 does not validate a file path before deleting it, nor does it restrict access to the relevant administration screens, allowing users with a role as low as Subscriber to delete arbitrary files on the server, which can lead to a full site compromise.	9.6	More Details
CVE-2026-115735	The Somatic Framework WordPress plugin through 1.8.14 does not perform an authorization check or validate a user-supplied file path before deleting it, allowing any authenticated user, such as a subscriber, to delete arbitrary files on the server, which can lead to a full site takeover.	9.6	More Details
CVE-2026-126872	Incorrect authorization in FileSystem in Google Chrome prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-126885	Use after free in ServiceWorker in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-107360	A flaw was found in rubygem-safemode. Compound assignment expressions in sandboxed code are evaluated without mediating method calls through the Jail allow-list. An authenticated attacker who can supply template content can invoke arbitrary no-argument methods on objects exposed to the template renderer without Jail mediation, including destructive operations such as host deletion and disclosure of non-allow-listed object state.	9.6	More Details
CVE-2026-126912	Buffer overflow in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-126842	Use after free in ANGLE in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-126164	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.	9.4	More Details
CVE-2026-68548	Algernon is a small self-contained pure-Go web server. Prior to version 1.17.10, Algernon's URL-prefix authorization gate matches its protected prefixes (/admin, /repo, /data) with case-sensitive strings.HasPrefix, while the exact same raw req.URL.Path is later resolved against the filesystem. On case-insensitive filesystems (Windows NTFS — always; macOS APFS/HFS+ — default), a request for /Admin/secret.lua evades every protected-prefix check, falls through to the public-prefix accept branch, and then resolves on disk to admin/secret.lua. The result is an unauthenticated bypass of the /admin, /repo, and /data authorization boundary, enabling read (and, for Lua files, execution) of protected content. The permission system is active in the default configuration. This issue has been patched in version	9.4	More Details

	1.17.10.		
CVE-2026-64670	Waline is a comment system with backend support. In versions 3.15.2 and prior, @waline/client renders the comment editor's live preview with marked and no sanitizer (utils/markdown.ts), and the preview is injected with v-html. When a comment is edited, the editor is seeded with the comment's raw, un-sanitized body (orig). Only administrators and the comment owner can edit. So an administrator who clicks Edit on an attacker's comment renders that attacker's raw HTML in their own session: an unauthenticated commenter achieves privilege-escalation stored XSS against a moderator with a single Edit click. At time of publication, there are no publicly available patches.	9.3	More Details
CVE-2026-124970	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP BASE WP BASE Booking wp-base-booking-of-appointments-services-and-events allows Blind SQL Injection.This issue affects WP BASE Booking: from n/a through 6.5.2.	9.3	More Details
CVE-2026-124415	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alejandro Alex Reservations alex-reservations allows SQL Injection.This issue affects Alex Reservations: from n/a through 2.4.8.	9.3	More Details
CVE-2026-126253	A authentication bypass by primary weakness vulnerability in Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13 may allow an unauthenticated attacker to broadcast LSA via specially crafted request	9.3	More Details
CVE-2026-126537	The Ninja Forms - File Uploads add-on for WordPress is vulnerable to Arbitrary File Deletion (and arbitrary file read via S3/Dropbox/Google Drive exfiltration) in versions up to, and including, 3.3.36. The flaw spans NF_FU_Fields_Upload::process() in includes/fields/upload.php — which returns early (leaving the client-supplied files[] intact) whenever a public submission carries a nonempty extra.saveProgress — and NF_FU_External_Abstracts_Service::process_upload() in includes/external/abstracts/service.php, whose authoritative-path reload only fires when the client sends upload_id. By omitting upload_id, an attacker's data[file_path] survives into the Background Upload queue and is used by both upload_file_to_s3() (as SourceFile) and the maybe_delete_server_file() unlink() call in includes/external/abstracts/backgroundupload.php, with no canonicalization or upload-directory containment check (the plugin's own is_path_within_upload_dir() helper is only applied on admin paths). This makes it possible for unauthenticated attackers to delete arbitrary files on the affected site's server which may make remote code execution possible — specifically, deleting wp-config.php forces WordPress into its setup screen, enabling full site takeover.	9.1	More Details
CVE-2026-129352	A vulnerability was detected in TRENDnet TEW-657BRM 1.00.1. This issue affects some unknown processing of the file /usr/sbin/upgrade_flash.cgi. Performing a manipulation of the argument boundary results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor explains: ""I am not able to confirm if such vulnerability exists as the product has been EOL for more than 15 years. We will send out an announcement letting customers know."	9.1	More Details
CVE-2026-122300	Missing Authorization vulnerability in Apache Roller 4.0 through 6.1.6 allows a weblog member with the Limited role to remove or change entries that member may only read, including entries published by other members. The entry editor checked the member's weblog role but not whether that role permits work on the entry. Users are recommended to upgrade to Apache Roller 6.1.7 or later.	9.1	More Details
CVE-2026-129258	A vulnerability was identified in Tenda AC18 15.03.05.05_multi/15.03.05.19 Build 6318. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/upgrade of the component Firmware Upgrade Handler. Such manipulation of the argument upgradeFile leads to insufficient verification of data authenticity. The attack may be launched remotely. The exploit is publicly available and might be used.	9.1	More Details
CVE-2026-85632	Missing authentication for critical function and Improper validation of integrity check value vulnerability in Sipay Electronic Money and Payment Services Inc. WooCommerce Virtual POS Module allows Authentication Bypass and Application API Message Manipulation via Man-in-the-Middle. This issue affects WooCommerce Virtual POS Module: from 26.8.3 before 26.9.1.	9.1	More Details
CVE-2026-129483	Cyrus SASL through 2.1.28 contains an authentication bypass vulnerability in the SRP server mechanism because srp_server_mech_step2 does not reject client public values A that are multiples of N. Unauthenticated network clients can send A equal to N to force a zero shared secret, authenticating as any existing user without the password and learning session keys.	9.1	More Details
CVE-2026-129452	A vulnerability has been found in DrayTek Vigor2960 1.5.1.6. This vulnerability affects the function set_table of the file /cgi-bin/mainfunction.cgi. Such manipulation of the argument jsondata leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.1.7 is able to resolve this issue. It is suggested to upgrade the affected component. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	9.1	More Details
CVE-2026-115733	The Printaura-Woocommerce WordPress plugin through 4.0.2 does not properly restrict access to the WooCommerce REST API, causing every WooCommerce REST route to accept unauthenticated requests, which allows unauthenticated attackers to read and modify store data including customer orders and personal information, store and payment settings, and webhooks.	9.1	More Details

CVE-2026-103813	Dell PowerStore contains an OS Command Injection vulnerability. An authenticated user with limited privileges could potentially exploit this vulnerability, potentially leading to privilege escalation to root on the appliance.	9.1	More Details
CVE-2026-129115	JSON::XS versions from 3.0 before 4.05 for Perl read freed stack memory when a FREEZE result's serialisation grows the Perl stack under allow_tags in encode_rv. With allow_tags, an object's FREEZE method is called in list context and each returned value is encoded through a saved Perl stack pointer. When encoding a returned value calls back into Perl, through TO_JSON under convert_blessed or another FREEZE, and that callback grows the stack, the stack is reallocated while the saved pointer still refers to the freed block. Encoding such objects reads freed memory, and encode can return undef without an error.	9.1	More Details
CVE-2026-129113	JSON::XS versions from 4.0_00 before 4.05 for Perl corrupt the incremental buffer length by chopping past its end in incr_skip after a top-level number. The incremental parser scans any run of digits, signs, dots and exponent markers as one number, but the decoder stops at the end of a valid number, so the parser keeps an offset into bytes it has not decoded. It then empties the buffer without clearing those bytes, and a later incr_parse call without new input reads them again and moves the offset past the end of the buffer. incr_skip, the documented recovery after an error, removes that many bytes and the buffer length wraps. A peer sending input such as "1-2" to an incr_parse consumer can make the next read of incr_text exit the process through perl's uncatchable out-of-memory path.	9.1	More Details
CVE-2026-124023	Out-of-bounds Read vulnerability in the Guththila XML parser wrapper of Apache Axis2/C. On some malformed XML input the Guththila parser returned a raw input byte in place of an event code, and the AXIOM reader wrapper used that value as an index into a ten-entry lookup table without checking its range, reading heap memory past the end of the table. An unauthenticated client could trigger this by sending a crafted XML request to a server built with Guththila, the default parser, causing the request to be parsed incorrectly or, in some cases, the process to crash. The memory read is not returned to the client. This issue affects Apache Axis2/C: through 2.0.0. The fix is available in commits 23110287924e79d05a5b4712298c355d1f05c606 and f01683ec10e8fddb87279ec9351b3239021223e6 and will be included in the next release.	9.1	More Details
CVE-2026-19422	Zohocorp ManageEngine DDI Central versions below 6301 is affected by an authentication bypass vulnerability in Windows DNS and DHCP agent synchronization APIs, allowing unauthenticated user to impersonate onboarded Windows servers and perform unauthorized DNS and DHCP modifications.	9.1	More Details
CVE-2026-124763	The Woocommerce Wishlist WordPress plugin through 1.1.0 does not have authorisation and CSRF checks in one of its unauthenticated AJAX actions, allowing unauthenticated users to overwrite any site option with the URL of an uploaded image or an empty value, breaking the site (for example by changing its URL or active , or deactivating every Woocommerce Wishlist WordPress plugin through 1.1.0).	9.1	More Details
CVE-2026-126378	Vvveb through 1.0.8.6 contains a file upload vulnerability in the theme installer validFile() function that uses strpos() instead of strict path matching. Attackers with admin credentials can upload a ZIP containing a PHP file whose path includes /theme.php to achieve remote code execution on nginx deployments.	9.1	More Details
CVE-2026-126380	Vvveb before 1.0.9.0 contains a denylist bypass in system/traits/media.php where '.phar' is misconfigured with a leading dot, allowing authenticated administrators to upload .phar PHP files. Attackers can upload a GIF magic-byte polyglot webshell bypassing binary inspection and execute arbitrary OS commands as the web-server user.	9.1	More Details
CVE-2026-126473	OpenEMR before 8.4.0 contains OAuth scope canonicalization and containment flaws that allow unauthenticated attackers to obtain unapproved system-level FHIR access. Attackers can register a colon-form system:Patient.read client that bypasses approval, then request unregistered system/Patient.write scope to read, modify, and create Patient records.	9.1	More Details
CVE-2026-126251	A incorrect authorization vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an attacker to bypass authentication and gain unauthorized access.	9.1	More Details
CVE-2026-126229	A authorization bypass through user-controlled key vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiAnalyzer Cloud 7.0 all versions, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager 7.0 all versions, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12, FortiManager Cloud 7.0 all versions may allow an authenticated administrator to access to other VDOMs via specially crafted HTTP requests.	9.1	More Details
CVE-2026-124014	XWEB EVO 4.3.0 through 5.8.8 contains an unauthenticated arbitrary file write vulnerability that allows remote attackers to modify the system configuration file /etc/xwebconfig.json by sending a crafted POST request to config.lua with action=set, which performs no session validation and writes the raw, unvalidated request body. Attackers can tamper with configuration values such as model and plugin fields or trigger a SYSTEM_NOT_CONFIGURED state via the unauthenticated action=get and action=set operations, resulting in configuration tampering and denial of service. This product line reached it's end of service date in March 2026.	9.1	More Details

CVE-2026-126157	A improper authentication vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to gain access to other users' secure email accounts via crafted HTTP requests.	9.1	More Details
CVE-2026-12507	Zohocorp ManageEngine AssetExplorer versions below 7860, ServiceDesk Plus versions below 15290, ServiceDesk Plus MSP versions below 15150, and SupportCenter Plus versions below 15150 are affected by a authenticated remote code execution vulnerability in the Reports module. An authenticated user with the Create Query Reports permission could exploit specially crafted database queries to execute arbitrary commands on the underlying server.	9.1	More Details
CVE-2026-126156	A authorization bypass through user-controlled key vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated remote attacker to take over an arbitrary IBE recipient account via crafted HTTP requests.	9.1	More Details
CVE-2026-126155	A incorrect authorization vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated remote attacker to obtain an authenticated IBE webmail session as any IBE recipient and read or send their encrypted mail via crafted HTTP requests.	9.1	More Details
CVE-2026-126150	A weak password recovery mechanism for forgotten password vulnerability in Fortinet FortiMail 8.0.0, FortiMail 7.6.0 through 7.6.5, FortiMail 7.4.0 through 7.4.7, FortiMail 7.2.0 through 7.2.9 may allow an unauthenticated attacker to reset the password of an arbitrary IBE webmail user and take over their account via specially crafted HTTP requests.	9.1	More Details
CVE-2026-129165	Tactical RMM 0.17.0 through 1.6.1 contains an arbitrary file read in the /reporting/templates/preview/ endpoint because WeasyPrint resolves file:// links in user-supplied template_md and embeds the files in the returned PDF. Users with report management permission can read the Django SECRET_KEY, reused as the NATS password, and publish runscript commands to every managed agent.	9.1	More Details
CVE-2026-116528	The Chargely Free Subscriptions For Woocommernce WordPress plugin through 1.0 does not perform any authorization check on a REST API route that returns its stored configuration, allowing unauthenticated attackers to retrieve the live WooCommerce REST API consumer key and secret it holds, which grant read and write access to the whole store.	9.1	More Details
CVE-2026-124539	JSON::XS versions before 4.05 for Perl leak the decoded key of an object rejected for a missing colon in decode_hv. Unless it is short plain ASCII, a quoted key is decoded into a new scalar. Nothing frees that scalar when the object is rejected for a missing ':' after the key. A process that keeps running after a failed decode retains one key per rejected document, with its size chosen by the sender. Repeated requests exhaust process memory.	9.1	More Details
CVE-2026-126325	A critical remote code execution (RCE) vulnerability has been reported in PTC Windchill and PTC FlexPLM. The vulnerability may be exploited through the deserialization of untrusted data.	9.0	More Details
CVE-2026-126257	A use of hard-coded password vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to bypass credential validation in certain circumstances outside of the attacker's control and gain unauthorized access.	9.0	More Details
CVE-2026-128049	OpenMage Magento LTS before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a cross-site request forgery vulnerability in the admin and storefront OAuth confirm and confirmSimple actions, which accept GET requests without form-key validation. Attackers holding OAuth consumer credentials can lure a logged-in administrator or customer to a crafted confirm URL that authorizes the attacker's request token, then exchange it at /oauth/token for a persistent REST API access token bound to the victim.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-91880	Dell Terraform Provider for PowerFlex, versions 1.5.0 through 1.8.0, contains an Improper Certificate Validation vulnerability in the SSH client component.Terraform PowerFlex provider uses ssh.InsecureIgnoreHostKey() as the default SSH host key callback. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	8.9	More Details
CVE-2026-126468	OpenEMR before 8.5.0 contains a missing authorization vulnerability that allows any authenticated low-privilege user to access reports, dated reminders, and batch reminder endpoints lacking AclMain::aclCheckCore() checks. Attackers can request patient_list.php, amc_full_report.php, dated_reminders_add.php, or batch_reminders.php directly to export patient PHI, send unauthorized reminders, and trigger batch reminder processing.	8.8	More Details
CVE-2026-125836	Cross-Site Request Forgery (CSRF) vulnerability in Nicu Micle Simple JWT Login simple-jwt-login allows Cross Site Request Forgery.This issue affects Simple JWT Login: from n/a through 3.6.8.	8.8	More Details
CVE-			

2026-125845	Cross-Site Request Forgery (CSRF) vulnerability in webriti vdequator vdequator allows Cross Site Request Forgery.This issue affects vdequator: from n/a through 1.2.7.	8.8	More Details
CVE-2026-76981	Zoho Corporation ManageEngine ADAudit Plus versions below 8711 are vulnerable to an authenticated second order SQL injection vulnerability affecting ADAudit Plus custom reports module.	8.8	More Details
CVE-2026-125844	Cross-Site Request Forgery (CSRF) vulnerability in webriti vice vice allows Cross Site Request Forgery.This issue affects vice: from n/a through 1.4.	8.8	More Details
CVE-2026-125843	Cross-Site Request Forgery (CSRF) vulnerability in webriti Spasalon spasalon allows Cross Site Request Forgery.This issue affects Spasalon: from n/a through 3.0.	8.8	More Details
CVE-2026-125842	Cross-Site Request Forgery (CSRF) vulnerability in webriti Wallstreet Agency wallstreet-agency allows Cross Site Request Forgery.This issue affects Wallstreet Agency: from n/a through 1.3.4.	8.8	More Details
CVE-2026-125841	Cross-Site Request Forgery (CSRF) vulnerability in webriti Heroic heroic allows Cross Site Request Forgery.This issue affects Heroic: from n/a through 1.4.2.	8.8	More Details
CVE-2026-125840	Cross-Site Request Forgery (CSRF) vulnerability in webriti Rambo rambo allows Cross Site Request Forgery.This issue affects Rambo: from n/a through 3.0.	8.8	More Details
CVE-2026-125839	Cross-Site Request Forgery (CSRF) vulnerability in webriti ElitePress elitepress allows Cross Site Request Forgery.This issue affects ElitePress: from n/a through 3.2.1.	8.8	More Details
CVE-2026-125838	Cross-Site Request Forgery (CSRF) vulnerability in webriti Quality quality allows Cross Site Request Forgery.This issue affects Quality: from n/a through 3.3.	8.8	More Details
CVE-2026-126868	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-125847	Cross-Site Request Forgery (CSRF) vulnerability in webriti vdperanto vdperanto allows Cross Site Request Forgery.This issue affects vdperanto: from n/a through 2.2.	8.8	More Details
CVE-2026-126869	Use after free in Frames in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126873	Use after free in Extensions in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126617	SQL injection in the database layer of Progressive Robot hMailServer 6.0.0-B1 through 6.2.18, when the server uses MySQL/MariaDB or PostgreSQL, allows a remote attacker to alter SQL statements the server runs. On those two engines parameters are not bound: SQLStatement::GenerateFromCommand wrote each value into the statement's text as a quoted literal with a separate string replacement over the whole text per parameter, so a value holding the name of a parameter substituted after it had that name replaced, inside the value, by the later value with its own quotes, which ended the literal early and placed the later value in the statement as SQL. The row the server writes for each recipient of a queued message carries the recipient's address twice, so in the default configuration an authenticated user who may send mail reaches it by sending to an address of their choosing. A remote unauthenticated sender reaches the same statement through a message the server sends to the envelope sender, such as a delivery failure notice or an automatic reply, and, when greylisting or message indexing is enabled (both are off by default), through the greylisting record's envelope addresses or through the message metadata the server stores for IMAP SORT, which carries four header fields of a received message. An altered statement runs with the privileges of the server's database account; on PostgreSQL, whose client call runs every statement in the text it is given, further statements can follow it, while on MySQL/MariaDB, where one statement is run per call, the change is confined to the statement it is in. SQL Server and SQL Server Compact, where parameters are bound, are not affected.	8.8	More Details
CVE-2026-128908	OS command injection (CWE-78) in the network-configuration handling of the management service (uavmonitor_usbv1) of the 1300 communications board in DJI AeroScope Mobile (TP703) firmware 03.00.00.26, with 1300 communications board firmware 02.00.07.12 through 02.00.08.40, allows an unauthenticated attacker on the local network to execute arbitrary commands as root. Configuration values that can be written without authentication over the management interface are inserted unquoted into shell commands. Exploitation requires network access to TCP port 16000 on the board and that the unit is not connected to another controlling host.	8.8	More Details

	The injected command persists across reboots. Confirmed on a physical device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. DJI has discontinued AeroScope Mobile and no fixed firmware is available.		
CVE-2026-128909	Improper verification of cryptographic signature (CWE-347) in the firmware update handler of the management service (uavmonitor_usbv1) of the 1300 communications board in DJI AeroScope Mobile (TP703) firmware 03.00.00.26, with 1300 communications board firmware 02.00.07.12 through 02.00.08.40, allows an unauthenticated attacker on the local network to install modified firmware, which gives persistent code execution as root. The device accepts any image that matches an MD5 checksum supplied in the same request and does not verify a signature. Exploitation requires network access to TCP port 16000 on the board and that the unit is not connected to another controlling host. Reproduced by running the unmodified device binaries in emulation; not tested on a physical device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. DJI has discontinued AeroScope Mobile and no fixed firmware is available.	8.8	More Details
CVE-2026-126874	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126876	Integer overflow in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-122003	The Abilities Bridge WordPress plugin before 1.4.2 does not require a valid nonce before re-authenticating a REST API request from the logged-in session cookie, allowing attackers to make a logged-in administrator perform any REST API action, including creating a new administrator account and taking over the site, by tricking them into opening a crafted page (CSRF).	8.8	More Details
CVE-2026-125846	Cross-Site Request Forgery (CSRF) vulnerability in webriti Mazino mazino allows Cross Site Request Forgery.This issue affects Mazino: from n/a through 1.1.	8.8	More Details
CVE-2026-12062	Zoho Corporation ManageEngine ADAudit Plus versions below 8703 are vulnerable to an authenticated SQL injection vulnerability in ADAudit Plus Reports API.	8.8	More Details
CVE-2026-126458	OpenEMR before 8.5.0 contains a missing authorization vulnerability in authorizations_full.php that allows any authenticated staff user to authorize arbitrary patients' clinical records. Attackers can send a mode=authorize request with an attacker-chosen pid and their own CSRF token to set authorized=1 on billing, forms, pnotes, and transactions records, bypassing provider review.	8.8	More Details
CVE-2026-125848	Cross-Site Request Forgery (CSRF) vulnerability in webriti Leo leo allows Cross Site Request Forgery.This issue affects Leo: from n/a through 1.7.4.	8.8	More Details
CVE-2026-126847	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126849	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126851	Use after free in Accessibility in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126466	OpenEMR before 8.5.0 contains a missing authorization vulnerability that allows any authenticated user to create patient records and enumerate patients by omitting aclCheckCore() checks. Attackers can POST to new_comprehensive_save.php to create patients with insurance PHI, or query new_search_popup.php and patient_select.php to leak names, SSNs and DOBs.	8.8	More Details
CVE-2026-126487	OpenEMR before 8.5.0 contains an authorization bypass vulnerability that allows authenticated users to override system-wide global configuration values by storing global-prefixed keys through library/ajax/user_settings.php. Attackers can submit lab or target parameters with global: prefixed setting names to disable audit logging, weaken password policies, or alter security-sensitive settings persistently for their sessions.	8.8	More Details
CVE-2026-126852	Use after free in MediaStream in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-19421	Zohocorp ManageEngine DDI Central versions below 6301 is affected by a PowerShell injection vulnerability due to insufficient validation of user-supplied TXT record values in Windows DNS operations.	8.8	More Details
CVE-	Incorrect authorization in FileSystem in Google Chrome prior to 157.0.8103.78 allowed a remote attacker		

2026-126860	leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-16135	The VibeBP plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.9.9.8.1. This is due to the plugin allowing arbitrary user meta updates through the set_email_notification_settings() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to grant themselves administrator privileges by updating their own 'wp_capabilities' user meta value.	8.8	More Details
CVE-2026-126861	Use after free in Media in Google Chrome on on Android prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-15309	The CourseCure Courses plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 1.5.1. This is due to a missing capability check in the ajax_save_settings() function, which accepts arbitrary POST parameters and calls update_option() with attacker-controlled keys and values without any authorization verification. This makes it possible for authenticated attackers, with subscriber-level access and above, to elevate their privileges to administrator by setting the default_role WordPress option to 'administrator' and users_can_register to '1', then registering a new account that is automatically granted full administrator access.	8.8	More Details
CVE-2026-13764	The Masterstudy - Education WordPress Theme theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.8.151. This is due to missing authorization and nonce validation on the `masterstudy_ms_stm_set_discard_transient` AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator by setting the `stm_developer_access_token` transient and using the developer access auto-login flow to obtain administrator session cookies.	8.8	More Details
CVE-2026-126863	Use after free in HTML in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126864	Use after free in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126865	Use after free in DOM in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126866	Incorrect authorization in Extensions in Google Chrome prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code inside the sandbox via a crafted Chrome extension. (Chromium security severity: High)	8.8	More Details
CVE-2026-126867	Use after free in Browser in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-125850	Cross-Site Request Forgery (CSRF) vulnerability in webriti Appointment Dark appointment-dark allows Cross Site Request Forgery.This issue affects Appointment Dark: from n/a through 1.3.4.	8.8	More Details
CVE-2026-125849	Cross-Site Request Forgery (CSRF) vulnerability in webriti Shk Corporate shk-corporate allows Cross Site Request Forgery.This issue affects Shk Corporate: from n/a through 2.4.3.	8.8	More Details
CVE-2026-126879	Use after free in Layout in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-126880	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-75869	Zohocorp ManageEngine DDI Central versions below 6301 is affected by an authorization bypass and PowerShell command injection vulnerability that allowed authenticated non-administrative users to target unauthorized Windows DHCP subnets and potentially execute arbitrary commands on managed Windows DHCP servers through crafted DNS suffix values.	8.8	More Details
CVE-2026-126905	Incomplete cleanup in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute		More

2026-126908	arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	Details
CVE-2026-126910	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126911	Use after free in Accessibility in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-126197	pgEdge Postgres MCP Server enables SQL queries against PostgreSQL databases through Model Context Protocol compatible clients. Prior to 1.1.0, custom pl-do tools interpolated JSON arguments into a PostgreSQL DO block delimited by fixed dollar-quote tags. An argument containing mcp_custom_tool could terminate the block and inject arbitrary SQL statements, while mcp_args could inject procedural code into a plpgsql block. Because the statement used the simple query protocol, injected text could include additional statements and transaction control, bypassing read_only and accessing data or modifying resources available to the connecting role. The issue requires at least one pl-do custom tool; sql and pl-func tools pass arguments as bind parameters and are not affected by this injection mechanism. This issue is fixed in 1.1.0.	8.8	More Details
CVE-2026-118411	Cross-Site Request Forgery (CSRF) in Apache Roller 5.0.1 through 6.1.6 allows an unauthenticated attacker to create an administrator account if a logged-in Roller administrator opens a link that the attacker controls. The request-token check applied only to POST requests, and administrative actions also accepted GET requests. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which requires POST and a valid token for actions that change data.	8.8	More Details
CVE-2026-86356	Dell PowerStore contains an authorization-bypass vulnerability that could lead to elevation of privilege to administrator.	8.8	More Details
CVE-2026-126916	Integer overflow in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-129123	C-Kermit 8.0.200 before 11.1.515 contains a buffer overflow vulnerability in getreply() in ckcftp.c that allows malicious FTP servers to overwrite client memory by sending overlong security replies. Attackers controlling or intercepting an FTP server can send long PBSZ replies after AUTH TLS, or long ADAT replies in GSSAPI, Kerberos 4, and SRP builds, overflowing the static reply_buf with attacker-controlled bytes.	8.8	More Details
CVE-2026-116615	The Widget Options – Advanced Conditional Visibility for Gutenberg Blocks & Classic Widgets plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 4.2.6.1 via the `post_content` parameter. This is due to asymmetric parsing between the save-time strip filter (`widgetopts_strip_logic_from_blocks()`) and the render-time parser (`blockopts_filter_before_display()`): embedding an inner `<!--start_widgetopts` literal inside a JSON key causes the write-side `json_decode` to see a non-`class` key and skip stripping — persisting the payload verbatim to the database — while the render-side `str_replace` reconstitutes the key to `class`, feeding the attacker-controlled `logic` value directly into `@eval`. This makes it possible for authenticated attackers, with Author-level access and above, to inject PHP expressions that execute on every front-end page view, enabling boolean-oracle exfiltration of WordPress site configuration data — including admin email address, default role, and arbitrary `get_option`, `get_user_meta`, and `get_post_meta` values — via the plugin's allowlisted-function sandbox, which escalates to unrestricted code execution if any installed plugin extends the `widgetopts_allowed_php_functions` filter. Contributors can also exploit this vulnerability when their submitted post is later published by an administrator; notably, the injected payload executes for all site visitors, including unauthenticated users, because a trust-flag mechanism introduced in version 4.2.6 causes `widgetopts_safe_eval_trusted()` to bypass its non-admin short-circuit at every legacy render callsite. Exploitation by attackers with contributor-level access and above requires that an administrator (or editor) later publishes the contributor's submission. On a default installation, where that is not configured, the vulnerability requires attackers with author-level access and above.	8.8	More Details
CVE-2026-123046	The SEOJuice WordPress plugin before 2.12.0 does not correctly restrict a REST API authentication filter, disabling WordPress's REST nonce protection for the whole site and allowing unauthenticated attackers to perform any cookie-authenticated REST action, including creating a new administrator account, by tricking a logged-in administrator into opening a crafted page (CSRF).	8.8	More Details
CVE-2026-123122	The Checkout Files Upload for WooCommerce WordPress plugin before 2.4.1 does not verify that a file uploaded at checkout is really one of its allowed image types, and serves stored uploads inline using their detected content type, allowing unauthenticated users to upload an HTML file disguised as an image that executes JavaScript in the browser of a shop manager or administrator who opens it from the order screen. This is a regression of CVE-2025-4212, reintroduced in 2.4.0.	8.8	More Details
CVE-2026-126917	Memory corruption in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-			

2026-126918	Use after free in Layout in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126919	Use after free in BrowserTag in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126921	Use after free in Accessibility in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-129255	A vulnerability was identified in CoolerMaster MASTERPLUS+ 1.9.6. This affects the function sub_11504 in the library WinRing0x64.sys of the component Device Driver. The manipulation of the argument PhysicalAddress leads to incorrect default permissions. The attack can only be performed from a local environment. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-18053	The MemberDash plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.8.7. This is due to a mass-assignment vulnerability in the `user_account_manager()` function's edit_profile branch, where all submitted `$_POST` fields are iterated and directly assigned to the current member object via the `MS_Model` `__set()` magic method with no field allowlist and no capability or ownership check on the submitted `id` parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject an arbitrary user ID via the `id` parameter — overwriting any WordPress user's email address and password, including the site administrator's — and subsequently use those modified credentials to gain full administrative access to the site.	8.8	More Details
CVE-2026-125784	Cross-Site Request Forgery (CSRF) vulnerability in Magnigenie RestroPress restropress allows Cross Site Request Forgery.This issue affects RestroPress: from n/a through 3.4.11.	8.8	More Details
CVE-2026-127090	Jadaptive Maverick Synergy Server before 3.0.33 and 3.1.x before 3.1.7, and Maverick Legacy Server before 1.8.1, contain an authentication bypass vulnerability in SSH public key authentication that reuses cached key authorization decisions across usernames. Attackers holding a key authorized for one account can authenticate it, then send a signed SSH_MSG_USERAUTH_REQUEST with a different username on the same connection to log in as that account.	8.8	More Details
CVE-2026-18379	A flaw was found in yggdrasil-worker-package-manager. An authenticated attacker can exploit this issue to achieve arbitrary file modification or potential privilege escalation. The vulnerability exists because repository management operations fail to sanitize directory traversal sequences (such as '../') within repository names. By supplying a crafted repository name, an attacker can manipulate the root-level worker process into creating or deleting files outside the intended directory, compromising host system integrity.	8.8	More Details
CVE-2026-116411	Dell PowerStore contains a Server-Side Request Forgery (SSRF) vulnerability. An authenticated user with limited privileges could potentially exploit this vulnerability, potentially leading to information disclosure via requests to internal services.	8.8	More Details
CVE-2026-126881	Improper initialization in Media in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-119615	The Reset Database plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.1.3. This is due to the process_reset() function being registered on admin_init with no capability check, a computed-but-unused nonce, a gating condition that passes whenever no WordPress administrator literally named 'admin' exists (the default on modern installs), and an identity test that verifies the ATTACKER'S OWN password rather than an administrator's. This makes it possible for authenticated attackers, with subscriber-level access and above, to drop every prefixed database table, re-run wp_install() with their own credentials — making the attacker the sole site administrator — authenticate as that administrator via wp_set_auth_cookie(), and delete the uploads directory.	8.8	More Details
CVE-2026-126886	Use after free in Frames in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126887	Use after free in Animation in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126888	Buffer overflow in Turbolev in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126889	Off-by-one error in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-126890	Out of bounds read in Media in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to potentially execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-125446	Cross-Site Request Forgery (CSRF) vulnerability in WisdmLabs Edwiser Bridge edwiser-bridge allows Cross Site Request Forgery.This issue affects Edwiser Bridge: from n/a through 4.3.4.	8.8	More Details
CVE-2026-126948	Zipline before 4.5.0 contains an insecure direct object reference vulnerability caused by missing ownership verification in the PATCH and DELETE handlers for /api/user/folders/:id. Authenticated attackers can supply another user's folder ID to rename it, make it public, enable uploads, or delete it.	8.8	More Details
CVE-2026-126892	Use after free in MediaStream in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-74857	A missing critical step in authentication vulnerability in the Auth API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write arbitrary files and conduct denial-of-service attacks.	8.8	More Details
CVE-2026-126893	Out of bounds write in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-18792	An improper limitation of a pathname to a restricted directory vulnerability in the Sharing API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write arbitrary files and conduct denial-of-service attacks.	8.8	More Details
CVE-2026-126895	Use after free in CSS in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-126897	Type confusion in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-13672	An authorization bypass through user-controlled key vulnerability in the SSOAuth in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write arbitrary files and conduct denial-of-service attacks.	8.8	More Details
CVE-2026-126899	Use after free in Elements in Google Chrome prior to 157.0.8103.78 allowed a remote attacker leveraging social engineering to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-126900	Use after free in CSS in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-103883	The 6Storage Rentals plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to, and including, 2.31.0. The vulnerability exists because the `six_storage_portal_registration()` AJAX handler — registered on `wp_ajax_six_storage_portal_plugin_registration` — performs no capability check and no nonce verification before writing the caller-supplied `six_storage_online_api_url` POST parameter to the site-wide option of the same name; the unauthenticated `six_storage_create_wp_user()` handler then redeems a transient seeded from that attacker-controlled URL's response and unconditionally calls `wp_set_current_user()` and `wp_set_auth_cookie()` with no ownership or credential verification. This makes it possible for authenticated attackers, with Subscriber-level access and above, to authenticate as any existing WordPress user — including any administrator whose email address is known or guessable — resulting in full site compromise. This issue represents an incomplete fix for a prior vulnerability: the 2.29.0 remediation moved the target email out of POST data into a server-side transient, but because any Subscriber can still overwrite the outbound API URL that populates that transient, the full authentication bypass chain remains exploitable in three AJAX requests.	8.8	More Details
CVE-2026-126901	Use after free in PDF in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-123769	The SureDash – Community, Courses & Member Dashboard plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.13.0 This is due to the `save_settings()` REST handler at `/suredash/v1/save-settings` being gated only by `admin_permission_callback()`, which authorizes any holder of the custom `manage_portal_dashboard` capability (Portal Manager role) without requiring `promote_users`, `edit_users`, or `manage_options`, combined with `sanitize_settings_data()` iterating all attacker-supplied keys with no allow-list, allowing arbitrary keys such as `default_role` to pass through `sanitize_text_field()` unchanged and be persisted into the `portal_settings` option via `update_option()` with no role-validity check. This makes it possible for authenticated attackers with Portal Manager-level access and above to poison the `default_role` setting to `administrator`, after which any subsequent new-user registration through the publicly	8.8	More Details

	accessible block-register endpoint reads the corrupted setting and passes it directly to `wp_insert_user()`, producing a full WordPress Administrator account under the attacker's control. The exploit requires two steps: a POST to the authenticated `save-settings` endpoint to overwrite `default_role`, followed by triggering a new registration through the unauthenticated block-register endpoint to receive the escalated account. Successful exploitation causes the attacker's own account to receive the complete administrator role.		
CVE-2026-126843	Type confusion in Turbolev in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-107524	Dell PowerStore contains an integer overflow vulnerability. An authenticated storage host could exploit this vulnerability, potentially leading to out-of-bounds data access or denial of service.	8.8	More Details
CVE-2026-82414	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. From versions 1.4.0 to before 1.4.6, 1.5.0 to before 1.5.1, and 1.6.0 to before 1.6.1, the BACnet MS/TP receive path decodes COBS frames into an output pointer inside the same fixed input buffer, but passes the full input-buffer size as the decode capacity. A long valid COBS payload can therefore write past the end of the actual remaining buffer. This issue has been patched in versions 1.4.6, 1.5.1, 1.6.1, and 1.7.0.	8.8	More Details
CVE-2026-97033	Building a malicious package that uses cgo could cause arbitrary code execution at build time through several compiler and linker flags permitted in "#cgo" directives. Specifically, "--sysroot" in GCC and Clang relocates compiler subprograms, spec files, and CRT startup objects to an attacker-controlled directory; "-target" in Clang falls back to executing target helper tools from the current working directory when not found in PATH; "-isysroot" and "-Wl,-syslibroot" can pass a regular file on disk to GNU ld.bfd, which interprets it as a positional linker script; and "-x" permitted specifying arbitrary compiler input languages beyond those supported by cgo. "--sysroot" and "-target" are now disallowed in "#cgo" flags, "-isysroot" and "-Wl,-syslibroot" are verified not to point to regular files, and "-x" is restricted to the C, C++, Objective-C, and assembler languages supported by cgo.	8.8	More Details
CVE-2026-116332	Use after free in PostgreSQL portal setup allows an object creator to execute arbitrary code as the operating system user running the database, via running user-defined code during planning or executor startup that closes the portal currently being prepared. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-127208	datamodel-code-generator before 0.84.0 contains a code injection vulnerability that allows attackers to achieve arbitrary code execution by supplying a malicious JSON Schema with a crafted x-python-type annotation containing a string ast.Constant node in a subscript slice position, which bypasses validation in parse_python_type_annotation and _python_type_expr_from_ast. Attackers can embed malicious Python expressions such as __import__ calls within quoted string literals in the generated source code, which Pydantic v2 evaluates as a ForwardRef via eval() during model_rebuild(), resulting in arbitrary code execution on developer workstations, CI/CD pipelines, or applications that generate and import the produced models at runtime.	8.8	More Details
CVE-2026-116331	Type confusion in PostgreSQL min/max aggregate optimization allows an object creator to execute arbitrary code as the operating system user running the database, via a user-defined aggregate whose SORTOP option causes the planner to treat the aggregate's input and result as the same type when they differ. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116330	Untrusted data inclusion in PostgreSQL pg_dump tar-format restore.sql allows a compromised origin server to execute arbitrary code as the client operating system account running psql, via the predictable restriction key in restore.sql. This is a gap in the fix for CVE-2025-8714. restore.sql is undocumented. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116329	Type confusion in PostgreSQL statistics import allows a table maintainer to execute arbitrary code as the operating system user running the database, via nested SET DATA TYPE during conversion of values to import. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are unaffected.	8.8	More Details
CVE-2026-116328	Integer wraparound in PostgreSQL generation memory contexts allows a database user to execute arbitrary code as the operating system user running the database, via freeing an allocation larger than 1 GB and causing its block to be reused for smaller chunks whose back-pointer offset cannot represent that position. Within major versions 16-18, minor versions before PostgreSQL 18.7, 17.12, and 16.16 are affected. Versions before PostgreSQL 16 are unaffected.	8.8	More Details
CVE-2026-116326	Uncaught exceptions in PostgreSQL plperl allow an object creator to cause use of a stale sigjmp_buf, via a tied Perl object, or a Perl object whose overloaded conversion throws while plperl is handling another error. We have not ruled out arbitrary code execution on some platform. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116323	Use after free in PostgreSQL pltcl allows an object creator to execute arbitrary code as the operating system user running the database, via a domain CHECK that re-enters the Tcl interpreter and frees or changes a string still used by the outer result conversion. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details

CVE-2026-97034	When using GCC, building a malicious package that uses cgo could cause arbitrary command execution at link time via untrusted GCC spec files ("specs" or "*.spec"). When linking with "-fopenmp", "-fopenacc", or "-fsanitize=" in "#cgo LDFLAGS", GCC's built-in link spec evaluates "%:include(libgomp.spec)" or "%:include(libsanitizer.spec)" and searches for spec files in "-L" and sysroot directories (including subdirectories and multilib sibling directories such as "../lib64"), as well as the working directory when "-fopenmp" or "-fopenacc" is used or when "-fsanitize=" is combined with "-static" or "-static-lib*". The go command now rejects "-L", "-isysroot", and "-Wl,-syslibroot" directories (and the working and package directories when applicable) that contain GCC spec files, and disallows "@" and "-" prefixes in "-fsanitize=" compiler flag values.	8.8	More Details
CVE-2026-86322	A flaw was found in Foreman’s Api::V2::PersonalAccessTokensController, where Foreman::Controller::UserAware#find_user resolves the target account using User.find(params[:user_id]) without applying the required parent-user authorization check. An attacker with the create_personal_access_tokens permission can therefore invoke POST /api/v2/users/:user_id/personal_access_tokens with another user’s ID and create a Personal Access Token on their behalf. The resulting plaintext token is returned in the API response, while PersonalAccessToken#check_permissions_after_save only validates create_personal_access_tokens on the token and does not enforce edit_users authorization on the target user. The attacker can then use the forged token to authenticate as the victim, potentially resulting in complete account takeover, including administrator accounts.	8.8	More Details
CVE-2026-97035	When using Clang or GCC, building a malicious package that uses cgo could cause unexpected code execution at build time or write files to arbitrary directories via "-gen-*" or "-gnat*" flags in "#cgo" directives. The "-g*" wildcard in the compiler and linker flag allowlists previously matched Clang's two-argument "-gen-cdb-fragment-path <dir>" flag and GCC's two-argument "-gnatO <file>" flag, permitting compilation database fragments and sidecar output files to be written to arbitrary directories and desynchronizing flag argument parsing between the go command and the compiler driver so that subsequent arguments could be passed as unvalidated positional inputs to the linker. "-gen-*" and "-gnat*" flags are now disallowed in "#cgo" compiler and linker flags.	8.8	More Details
CVE-2026-97036	On Darwin, building a malicious package that uses cgo could cause arbitrary code execution when using the Apple linker due to passing "-l to_library <path>" in a "#cgo LDFLAGS" directive. The Apple linker recombines the separated arguments "-l" and "to_library" into "-lto_library", which loads an arbitrary LTO plugin dynamic library at link time. The go command now disallows "-l" followed by "to_library" in "#cgo LDFLAGS", rejects "-lazy_library", "-lazy_framework", "-load_hidden", "-library", and "-library-path", and checks recombined "-l" arguments against disallowed linker flags and patterns.	8.8	More Details
CVE-2026-97037	Building a malicious package that uses cgo could cause arbitrary code execution at link time by passing linker script files to the host linker via "#cgo LDFLAGS". Split "-Wl," flags that consume a following argument (such as "-Wl,-rpath", "-Wl,--just-symbols", and "-Wl,-undefined") previously accepted a bare second argument without a "-Wl," prefix, which the compiler driver passes directly to the linker as a positional input file. Additionally, when using GNU ld.bfd, flags such as "-framework", "-Wl,-framework", "-Wl,-undefined", "-Wl,--just-symbols", "-Wl,-R", "-Wl,-subsystem", and (on non-Darwin platforms) "-Wl,-sectcreate" could cause ld.bfd to interpret their arguments as linker scripts if they named a regular file on disk. The go command now requires a "-Wl," prefix on the second token of split "-Wl," flags (except "-Wl,-R"), verifies that these flags do not reference linker script files, and disallows bare "-Wl,--warn-backrefs-exclude".	8.8	More Details
CVE-2026-97038	Building a malicious package containing ".syso" files or cgo linker inputs could inject arbitrary linker flags or execute arbitrary code at link time. Linker input files—including ".syso" files, direct object or library inputs in "#cgo LDFLAGS", and libraries in "-L" directories—were passed to the external linker without validating their format or checking for embedded linker options. Across platforms, this allowed executing GNU ld implicit linker scripts disguised as libraries or ".syso" files (or loaded via "-l:<filename>" or "-l" containing path separators), injecting unallowlisted linker flags via PE/COFF ".drectve" sections on Windows or Mach-O "LC_LINKER_OPTION" load commands on Darwin, or invoking LTO plugins via GCC or LLVM LTO intermediate representation sections in ELF, PE/COFF, or Mach-O objects. The go command now verifies that ".syso" files, direct linker inputs, and libraries in "-L" directories are valid binary objects or archives that do not contain unallowlisted ".drectve" directives, "LC_LINKER_OPTION" load commands, or LTO IR sections, and disallows "-l:<filename>" and ":", "=", or path separators in "-l" flags.	8.8	More Details
CVE-2026-91879	Dell Terraform for ObjectScale and Powerstore, versions prior to 1.1.1 (ObjectScale) and versions 1.2.1 through 1.3.0 (PowerStore) contains an insertion of sensitive information into Log File vulnerability in the client initialization component. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	8.8	More Details
CVE-2026-97041	Building a malicious package containing "//go:cgo_*" compiler directives could inject arbitrary flags into the external linker invocation on ELF platforms. The compiler and linker did not reject commas in "//go:cgo_import_dynamic", "//go:cgo_export_dynamic", "//go:cgo_export_static", "//go:cgo_import_static", and "//go:cgo_dynamic_linker" directives, and the linker passed the dynamic linker path using "-Wl,--dynamic-linker, <path>". Furthermore, the two-argument form of "//go:cgo_import_dynamic" (which is permitted in non-cgo Go source files) could overwrite the external symbol name of a symbol already marked for cgo export. A symbol name or dynamic linker path containing a comma or leading "@" could split "-Wl,--export-dynamic-symbol=" or "-Wl,--dynamic-linker," into arbitrary host linker flags or response file arguments. The compiler and linker now reject commas in "//go:cgo_*" symbol and dynamic linker directives, the linker passes "-Wl,--dynamic-linker= <path>", and "cgo_import_dynamic" no longer overwrites symbols exported via "cgo_export_dynamic" or "cgo_export_static".	8.8	More Details

CVE-2026-97042	Building a malicious package that uses "//go:cgo_import_dynamic" or links against a crafted PE object on Windows could pass unsafe library arguments to the external linker. The compiler only checked the first character of the library name in "//go:cgo_import_dynamic" directives and skipped validation in cgo-generated files. In addition, on Windows, "cmd/cgo" and "cmd/link" did not validate imported DLL names extracted from PE object files before emitting "-l<name>" flags for the external linker, allowing a crafted DLL name containing ".." path traversal or special characters to reference arbitrary files on disk. The compiler now validates every character of the library name in "//go:cgo_import_dynamic" directives (including in cgo-generated files on Windows) and rejects ".." path traversal, and "cmd/cgo" and "cmd/link" reject PE imported DLL names containing path separators, "..", ":", or leading "-" or "@".	8.8	More Details
CVE-2026-126840	Out of bounds write in Network in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-116335	Type confusion in PostgreSQL operator commutator and negator links allows an object creator to execute arbitrary code as the operating system user running the database, via linking operators having different result types or creating inconsistent reciprocal links. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126370	Vvveb through 1.0.8.6 contains a remote code execution vulnerability allowing restricted site_admin roles to inject PHP by saving .sql files through the admin code editor. Attackers can bypass extension and content deny-lists with an @IF macro payload that compiles into executable PHP when the model loads, running OS commands as the web user.	8.8	More Details
CVE-2026-129465	Zr.Admin.NET commit af07ffc through commit eb9228a contains an insecure direct object reference vulnerability in SysProfileController.UpdateProfile that allows any authenticated user to modify other accounts via UserId. Attackers can set the administrator's phone number to one they control, request an SMS code via /checkMobile, and log in through /PhoneLogin to take over the administrator account.	8.8	More Details
CVE-2026-126801	Rote 1.2.0 through 2.6.0 contains an authorization bypass in the OAuth bind/merge endpoint that allows authenticated users to merge any OAuth-bound account into their own. Attackers can submit a public existingUserId and GitHub or Apple user ID to take over notes, attachments, and API keys and delete the victim account.	8.8	More Details
CVE-2026-126317	Frappe HRMS from 16.0.0 before 16.20.1 contains a missing authorization vulnerability that allows authenticated users to read company details outside their permissions due to a missing permission check. Any logged-in user, including Employee role users, can query the affected endpoint to list every company on the site along with its default currency.	8.8	More Details
CVE-2026-126469	OpenEMR before 8.5.0 contains a missing authorization vulnerability in several custom/ scripts that rely only on session authentication and never call AclMain::aclCheckCore(). Any authenticated low-privilege user can request export_labworks.php, chart_tracker.php, or export_registry_xml.php to disclose patient SSN, DOB, and insurance data or provider NPI/tax IDs, and forge chart-tracker records.	8.8	More Details
CVE-2026-100307	Missing authorization in the external management API in Amazon mcp-gateway-registry 1.0.9 through 1.24.7 might allow an authenticated remote user to assign the registry administrator scope to their own identity group and obtain administrative control of every registered gateway asset via a crafted group import request. To remediate this issue, users should upgrade to version 1.25.0.	8.8	More Details
CVE-2026-120151	Type confusion in PostgreSQL plpgsql record-field assignment allows an object creator to execute arbitrary code as the operating system user running the database, via a reentrant domain CHECK that changes a RECORD variable's row type while a value is being cast. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-120150	Use after free in PostgreSQL expanded-record domain checks allows an object creator to execute arbitrary code as the operating system user running the database, via repeated checks of a domain over a composite type that cause reuse of a dangling memory-context pointer. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126314	Frappe HRMS 15.0.0 before 15.64.6 and 16.0.0 before 16.20.1 does not check access to each employee on endpoints that create records in bulk for a list of employees. An authenticated user with create permission on the affected record type, such as HR User, can create records for employees outside their user-permission scope, including other companies' employees.	8.8	More Details
CVE-2026-125449	Deserialization of Untrusted Data vulnerability in Mamunur Rashid Testimonial Slider testimonial-slider-and-showcase allows Object Injection.This issue affects Testimonial Slider: from n/a through 3.0.2.	8.8	More Details
CVE-2026-120149	Heap-based buffer overflow in PostgreSQL foreign batch inserts allows a foreign server to execute arbitrary code, via reporting that it inserted more rows than the server supplied. postgres_fdw can legitimately encounter this when a rule on the remote table expands an INSERT into additional rows. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-	Use after free in the PostgreSQL dblink extension allows an object creator to execute arbitrary code as the		

2026-120147	operating system user running the database, via type conversion code that re-enters dblink and closes a connection whose results an outer dblink call is reading. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116336	Operation on a dropped index in PostgreSQL REINDEX CONCURRENTLY allows an object creator to execute arbitrary code as the operating system user running the database, via an index expression that issues DROP INDEX. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126470	OpenEMR before 8.5.0 contains an insecure direct object reference vulnerability in the Carecoordination module that allows authenticated users with send_to_hie permission to access any patient's CCDA/CCR/QRDA documents. Attackers can supply arbitrary document or patient IDs to download, transmit, or export patient health records, inject falsified clinical data, and delete audit records.	8.8	More Details
CVE-2026-120145	Missing authorization in PostgreSQL logical replication allows a compromised publisher to execute arbitrary code as the operating system user running the superuser-owned subscription, via naming a system catalog as a replication target. Only subscriptions owned by a superuser are vulnerable. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-111545	Dell PowerStore contains a SQL Injection vulnerability. An authenticated attacker could exploit this vulnerability, potentially leading to disclosure of stored private keys and tampering with trusted certificates.	8.8	More Details
CVE-2026-120144	Type confusion from incomplete PostgreSQL type-cache invalidation allows an object creator to execute arbitrary code as the operating system user running the database, via a composite type change while its cache entry is being populated. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are unaffected.	8.8	More Details
CVE-2026-120143	Use after free in PostgreSQL trigger functions allows an object creator to execute arbitrary code as the operating system user running the database, via a cursor over a transition table. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-120142	Type confusion in PostgreSQL anonymous RECORD types allows an object creator to execute arbitrary code as the operating system user running the database, via row types having dropped attributes in the same positions but with different widths or alignments. Within major versions 17-18, minor versions before PostgreSQL 18.7 and 17.12 are affected. Versions before PostgreSQL 17 are unaffected.	8.8	More Details
CVE-2026-120141	Type confusion in PostgreSQL materialized set-returning functions allows a database user to execute arbitrary code as the operating system user running the database, via returning rows having different dynamic RECORD return types. json_populate_recordset() is one affected function. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-120139	Integer wraparound in PostgreSQL in-memory tuple-size calculations allows a database user to execute arbitrary code as the operating system user running the database, via oversized tuple data. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126472	OpenEMR before 8.5.0 contains a missing authorization vulnerability in ccdaservice/ccda_gateway.php that allows any authenticated low-privilege staff user to retrieve other patients' C-CDA documents. Attackers can request the view or dl action with sequential pid values and their own CSRF token to enumerate and exfiltrate medications, problems, allergies, and immunizations.	8.8	More Details
CVE-2026-97043	Building a malicious package that uses cgo could bypass "#cgo LDFLAGS" validation and cause unexpected code execution at build time, or cause the go command to panic, via crafted quoting in "//go:cgo_ldflag" directives. When "cmd/cgo" generates "_cgo_gotypes.go", it quotes each "#cgo LDFLAGS" argument with strconv.Quote in a "//go:cgo_ldflag" directive, but "cmd/compile" and "cmd/go" parsed those directives by splitting on raw quote characters without handling backslash escapes or unquoting the string. This mismatch allowed disallowed linker flags or unvalidated linker search paths to be smuggled past the go command's flag checks and passed to the external linker. In addition, deduplicating LDFLAGS in the go command could panic with an out-of-bounds slice index when a prefix of the flag list matched near the end of the slice. "cmd/compile" and "cmd/go" now properly handle backslash-escaped quotes and unquote "//go:cgo_*" pragma strings with strconv.Unquote, and the slice bounds check in processCgoOutputs has been fixed.	8.8	More Details
CVE-2026-116320	Use after free in PostgreSQL plperl allows an object creator to execute arbitrary code as the operating system user running the database, via dropping the final reference to a Perl array or hash while PostgreSQL is converting that object. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116307	Use after free in PostgreSQL plperl allows an object creator to execute arbitrary code as the operating system user running the database, via re-entering plperl and freeing a prepared query while an outer invocation is executing it. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116319	Use after free in PostgreSQL plperl allows an object creator to execute arbitrary code as the operating system user running the database, via reentrant return_next() calls. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-	Deserialization of Untrusted Data vulnerability in VillaTheme AFFI – Affiliate Marketing for WooCommerce affi-		

2026-120835	affiliate-marketing-for-woo allows Object Injection.This issue affects AFFI – Affiliate Marketing for WooCommerce: from n/a through 1.0.11.	8.8	More Details
CVE-2026-126283	NocoDB before 2026.08.0 contains an incorrect authorization vulnerability that lets base-scoped API tokens act as account-wide credentials because the token's base_id is never stored or checked. Attackers holding a leaked token can read, write and delete records on every base the token owner belongs to, including bases joined later.	8.8	More Details
CVE-2026-126241	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an authenticated attacker to execute unauthorized SQL commands on the underlying database.	8.8	More Details
CVE-2026-106152	In Progress® Telerik® Report Server prior to version 12.3.26.1110, an external control of a system configuration setting vulnerability allows an unauthenticated remote attacker to influence the server address used by Report Server when generating links and notifications. With user interaction, this can lead to disclosure of sensitive information and account takeover.	8.8	More Details
CVE-2026-126723	Rooxis RXR-12 Wi-Fi router contains an authenticated command injection vulnerability in the LuCI white_list RPC handler (/usr/lib/lua/luci/data/white_list_plt.lua), where unsanitized user-supplied MAC addresses are concatenated into os.execute() without validation, yielding root command execution via a malformed mac parameter. Firmware 20260813_c2169ea5 fixes the vulnerability, and users can update their router through the local web interface.	8.8	More Details
CVE-2026-119512	Deserialization of Untrusted Data vulnerability in Tribulant Software Newsletters newsletters-lite allows Object Injection.This issue affects Newsletters: from n/a through 4.18.2.	8.8	More Details
CVE-2026-121862	The Knowledge Building WordPress plugin before 0.7.3 does not sanitise and escape comments submitted through its reply feature, and publishes them without moderation, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against any visitor of the affected posts, including administrators.	8.8	More Details
CVE-2026-129464	Zr.Admin.NET commit 0ee1ab8 through commit eb9228a contains a path traversal vulnerability that allows any logged-in user to read arbitrary server files via the path parameter of /common/DownloadFile. Attackers can supply absolute paths or ../ sequences to read appsettings files and use the JwtSettings SecretKey to forge administrator tokens.	8.8	More Details
CVE-2026-67543	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.70, heym hardens one untrusted-code path but not its sibling. The Python tool executor (python_tool_executor.py) treats user code as untrusted and mandates a Docker sandbox (no network, read-only fs, non-root, no docker socket), failing closed. The skill executor (skill_python_executor.py) runs skill Python via a local backend subprocess with no Docker isolation — only a 512 MB RLIMIT and a 7-key env denylist — so a skill executes inside the backend execution context, with filesystem access, network egress, and non-denylisted environment variables that should not be exposed to untrusted/shared skills. In the shipped Docker config (backend runs as root + /var/run/docker.sock mounted), this escalates to host root. This issue has been patched in version 0.0.70.	8.8	More Details
CVE-2026-67544	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.71, Heym's workflow engine accepts an arbitrary Python code string in the playwrightCode field of a Playwright node. This string is written to a temporary .py file and executed directly by the backend process via subprocess.Popen([sys.executable, script_path]) with no sandboxing, AST validation, or role gate. Any authenticated user — including a freshly registered account — can achieve full remote code execution (RCE) on the backend host, running as the service process user (observed as root in the default Docker deployment). This issue has been patched in version 0.0.71.	8.8	More Details
CVE-2026-121998	The iChart WordPress plugin before 2.2.4 does not perform capability or ownership checks in several of its AJAX actions, relying only on a nonce that any logged-in user can obtain, allowing users with a role as low as Subscriber to read, modify and permanently delete arbitrary posts and to overwrite a site-wide option.	8.8	More Details
CVE-2026-67546	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.75, the same POST /api/mcp/fetch-tools endpoint (any authenticated user, lowest role) also accepts the stdio transport, which spawns the attacker-supplied command with attacker-supplied args and an environment merged over os.environ. The process executes on the shared backend host before MCP protocol validation fails — so side effects fire regardless of whether the command speaks MCP. This is a distinct weakness class and exploit primitive from the SSRF (Advisory 2) on the same endpoint, and needs a different fix (role gating / opt-in trust boundary rather than egress controls). This issue has been patched in version 0.0.75.	8.8	More Details
CVE-2026-67547	taOS is a self-hosted AI agent OS. Prior to version 1.0.0-beta.23, the POST /api/skill-exec/{skill_id}/call endpoint in taOS executes built-in skills — including the code_exec skill which runs arbitrary Python via subprocess.run(["python3", "-c", code]) — without performing any admin role check, skill ownership check, or agent assignment verification. Any authenticated non-admin user can supply attacker-controlled Python code in the request body and have it executed as the taOS backend process user on the host, achieving full remote code execution with no privilege escalation required beyond a valid (non-admin) session. This issue has been patched in version 1.0.0-beta.23.	8.8	More Details

CVE-2026-123134	The Smoove abandoned cart trigger for WooCommerce WordPress plugin before 4.3.6 does not sanitise and escape abandoned-cart data submitted by visitors before outputting it in the admin dashboard, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against administrators.	8.8	More Details
CVE-2026-124013	XWEB EVO 5.6.2 through 5.8.8 contains an authenticated OS command injection vulnerability in the api.lua import_preconfiguration and restore actions, where server_url and related server credential fields are concatenated unescaped into a root curl command executed via io.popen. Attackers can inject malicious shell commands through these unfiltered parameters to achieve arbitrary command execution with root privileges on the underlying system. This product line reached it's end of service date in March 2026.	8.8	More Details
CVE-2026-126482	OpenEMR before 8.5.0 contains an SQL injection vulnerability in SLEOB::slInvoiceNumber() in src/Billing/SLEOB.php, which concatenates the CLP01 claim identifier from uploaded X12 835 ERA files into a query without escaping or parameter binding. Authenticated users with billing permissions, or a malicious payer whose ERA file a clerk uploads, can execute arbitrary SQL to read any table, including users_secure password hashes, and modify data.	8.8	More Details
CVE-2026-116306	Type confusion in PostgreSQL composite-value field assignment allows an object creator to execute arbitrary code as the operating system user running the database, via changing a composite type between deforming and reforming a value. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116304	Use after free in PostgreSQL coordination of anonymous RECORD type identifiers among parallel workers allows a database user to execute arbitrary code as the operating system user running the database, via causing one process to free a shared tuple descriptor while another process retains and later uses its address. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-125423	A repository created with auto-init accepted pushes before its initialization had finished, and the initial commit was built in a checkout of whatever the repository already contained. A user who is allowed to create repositories could push a crafted tree during that window so that writing the README followed a symbolic link and overwrote a server-side git hook, which runs commands as the Gitea system user. The initial commit is now built in a freshly initialized directory, and a new repository only becomes ready, and accepts pushes, once its initialization is complete.	8.8	More Details
CVE-2026-126175	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.2 through 7.2.12, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.2 through 7.2.13, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.2 through 7.2.12, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.2 through 7.2.13 may allow an authenticated attacker to execute unauthorized code or commands via crafted JSON-RPC requests.	8.8	More Details
CVE-2026-126372	Vvveb through 1.0.8.6 contains an incomplete fix for CVE-2026-41934 that allows authenticated editor or site_admin users to write server-side templates by bypassing save restrictions. Attackers can upload or rename .tpl files via editor/code upload and rename actions, or evade isExecutableFile checks in save(), to inject PHP code into templates.	8.8	More Details
CVE-2026-116318	SQL injection in PostgreSQL pg_dump allows an object creator to execute arbitrary SQL as the user restoring the dump, via an inherited column having a child-local not-null constraint whose name requires quoting. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are unaffected.	8.8	More Details
CVE-2026-116317	Heap-based buffer overflow in PostgreSQL ts_rank_cd() may allow a database user to execute arbitrary code as the operating system user running the database, via an invalid tsvector containing duplicate positions. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126144	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.4, FortiMail 7.4.0 through 7.4.6, FortiMail 7.2 all versions, FortiRecorder 7.6.0 through 7.6.2, FortiRecorder 7.2.0 through 7.2.12, FortiRecorder 7.0.0 through 7.0.6 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	8.8	More Details
CVE-2026-126291	NocoDB before 2026.06.2 contains an SQL injection vulnerability in base-user.cte.utils.ts, which concatenates base members' email addresses into the SQL text of queries resolving user, created-by or last-modified-by fields. Registered users can set an email with a quoted local part containing a single quote to execute arbitrary SQL, exposing user records, API tokens and data-source credentials.	8.8	More Details
CVE-2026-116316	Improper protection of alternate path in PostgreSQL security-restricted operations allows an object creator to execute arbitrary SQL as the operation's caller, via a domain, enum, or range type created in pg_temp. The victim session must later run a query containing an unqualified type name, e.g. "SELECT '1'::bigint"; autovacuum and other common security-restricted operation users do not do so, so they are unaffected. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116315	Heap-based buffer overflow in PostgreSQL tsvector_delete() allows a database user to execute arbitrary code as the operating system user running the database, via a tsvector whose lexeme data uses a nonstandard but valid ordering that requires additional alignment padding in the result. Versions before PostgreSQL 18.7, 17.12, 16.16,	8.8	More Details

	15.20, and 14.25 are affected.		
CVE-2026-118041	The Contest Gallery WordPress plugin before 34.0.3 does not sanitise the name of files uploaded through its e-commerce sale file-replacement feature, allowing authenticated users with Author-level access and above to write files with an arbitrary name and extension to a web-accessible directory and, by overwriting the directory's protection file through the same flow, achieve Remote Code Execution.	8.8	More Details
CVE-2026-126414	Frappe HRMS 15.0.0 before 15.64.2 and 16.0.0 before 16.20.0 contains a missing authorization vulnerability in certain record update endpoints that lack an ownership check. Authenticated users with the Employee role can call these endpoints to modify records belonging to other employees, beyond their permitted role.	8.8	More Details
CVE-2026-116314	Improper input validation in PostgreSQL pg_restore allows a non-plain archive provider to execute arbitrary code as the operating system user running pg_restore, via a crafted archive. Note a contrast: crafted archive data may legitimately cause arbitrary SQL to execute at the restore destination, but it does not legitimately confer arbitrary code execution in the pg_restore OS process. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-18447	Type confusion in PostgreSQL SQL-language functions allows an object creator to execute arbitrary code as the operating system user running the database, via an output parameter of type "any". Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-6460	Type confusion in PostgreSQL allows an object creator to execute arbitrary code as the operating system user running the database, via ALTER ... SET DATA TYPE primarily. Other DDL attack routes exist, such as "ALTER TABLE ... ADD COLUMN; ROLLBACK; ALTER TABLE ... ADD COLUMN". The system had inadequate tracking of typed values, and values were not self-identifying. Stale values could appear in data dictionary entries, PL/pgSQL variables, and many other parts of the system. PostgreSQL Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-116309	Type confusion in PostgreSQL plperl may allow an object creator to execute arbitrary code, via blessing a non-hash reference into PostgreSQL::InServer::ARRAY. We have not confirmed or ruled out a way to control the pointer sufficiently to achieve security impact, but we are proceeding as though that is possible. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.8	More Details
CVE-2026-126412	Frappe HRMS 15.0.0 before 15.64.1 and 16.0.0 before 16.19.0 lacks a write permission check on a bulk record processing action, allowing users with only read access to the related setup record to modify data. Authenticated users with the default Employee role can run the action to create and submit records for every covered employee.	8.8	More Details
CVE-2026-118389	The RubyGems package registry accepted gems whose platform, dependency names or dependency version requirements contain newline characters. Because the compact index served to clients is line-based, a user who can publish a gem to an owner's registry could forge index entries, such as packages that do not exist or additional versions of an existing gem with dependencies of their choice. Clients that resolve gems from that registry could then be led to install attacker-chosen dependencies. Gems with such metadata are now rejected.	8.8	More Details
CVE-2026-126785	A vulnerability has been found in rmalright TR-VISION HOME 2.0.5. Impacted is the function sub_11504 in the library WFanManager.sys of the component IOCTL Handler. Such manipulation leads to incorrect default permissions. The attack must be carried out locally. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-91890	Dell Ansible Storage for Unity , versions prior to 1.2.13 contains an Improper Certificate Validation vulnerability in the UnityRESTConnector component. An unauthenticated attacker with remote access could potentially exploit this vulnerability,leading to information exposure and unauthorized access.	8.7	More Details
CVE-2026-126806	WWBN AVideo 14.3 through 29.7.1 contains a stored cross-site scripting vulnerability that allows uploaders to inject scripts via the videoDownloadedLink value stored unescaped through objects/aVideoEncoder.json.php. Attackers can embed event-handler payloads in the URL host rendered as a Source tag in view/managerVideos_body.php, executing in administrator sessions to install plugin archives containing PHP.	8.7	More Details
CVE-2026-126162	A xml injection (aka blind xpath injection) vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6 may allow a remote unauthenticated attacker to execute unauthorized code or commands via a specially crafted request.	8.7	More Details
CVE-2026-126800	Hydro @hydrooj/ui-default before 4.59.1 contains a stored cross-site scripting vulnerability that allows registered users to inject script by placing double quotes in language- class tokens within markdown-it-xss.ts. Attackers can store a payload in their profile bio that executes when administrators or other users view it, stealing the non-httpOnly sid session cookie for session hijacking.	8.7	More Details
CVE-2026-126217	A incorrect authorization vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to escalate their privileges, bypass authorization controls or impersonate internal services via specially crafted requests to the GUI.	8.7	More Details

CVE-2026-126183	A authorization bypass through user-controlled key vulnerability in Fortinet FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker to execute commands outside of the expected scope via specially crafted HTTP request.	8.7	More Details
CVE-2026-91875	Dell OpenManage Ansible Modules, versions 9.2.0 through 10.0.3, contains an Improper Certificate Validation vulnerability in the SessionAPI component. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	8.7	More Details
CVE-2026-91874	Dell OpenManage Ansible Modules, versions 5.0.0 through 10.0.3, contains an Improper Certificate Validation vulnerability in the iDRACConnection component. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	8.7	More Details
CVE-2026-91873	Dell OpenManage Ansible Modules, versions 2.1.2 through 10.0.3, contains an Improper Certificate Validation vulnerability in the iDRACRedfishAPI component. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	8.7	More Details
CVE-2026-126274	NocoDB before 2026.08.0 contains a stored cross-site scripting vulnerability that allows authenticated Creator users to inject script by embedding markup in column or table titles. The Delete.vue confirmation dialog renders these titles through an unescaped innerHTML binding, executing script when a victim deletes an external-source table to steal session tokens from localStorage.	8.7	More Details
CVE-2026-107523	Dell PowerStore contains an integer overflow vulnerability. An adjacent attacker could exploit it to bypass volume bounds checks, potentially leading to data destruction or denial of service.	8.7	More Details
CVE-2026-126269	NocoDB before 2026.09.0 contains a stored cross-site scripting vulnerability that allows authenticated Editor users to execute scripts by storing crafted attachment MIME types like text/html;image/png. Attackers can write the value through the records API so the /dltemp signed URL serves HTML inline, stealing session tokens from localStorage to impersonate victims.	8.7	More Details
CVE-2026-126310	OpenBao before 2.6.5 and 2.7.2 contains an authentication bypass vulnerability that allows unauthenticated callers to obtain OIDC ID tokens by abusing public clients with client_credentials enabled. Attackers who know a public client's client_id can request tokens from the identity/oidc/provider/<name>/token endpoint to impersonate the client without any secret.	8.7	More Details
CVE-2026-129427	Stored XSS via avatar upload chained with an authentication bypass in /Attachments leads to ATO in Cervantes version v1.3-beta could allow an attacker to execute arbitrary code in another user's browser with elevated privileges	8.7	More Details
CVE-2026-126945	Zipline before 4.5.1 contains a stored cross-site scripting vulnerability in the HighlightCode component that renders unescaped file content before highlight.js finishes loading. Authenticated attackers can upload text files containing HTML/JavaScript payloads that execute in viewers' browsers, enabling API calls such as account changes on the victim's behalf.	8.7	More Details
CVE-2026-49990	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. From versions 1.4.2 to before 1.4.5, and 1.5.0 to before 1.5.1, a signed fileStartPosition taken from AtomicReadFile and AtomicWriteFile stream-access requests is not validated tightly enough before it reaches the RAM file backends. Practical impact includes: reliable denial of service via process crash, out-of-bounds read that may expose adjacent memory contents, or out-of-bounds write that may corrupt heap memory and destabilize the process. This issue has been patched in versions 1.4.5 and 1.5.1.	8.6	More Details
CVE-2026-124647	The TI WooCommerce Wishlist WordPress plugin before 2.0.7 does not sanitise and escape user input before using it in a SQL statement in a front-end endpoint, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-106146	In Progress® Telerik® UI for ASP.NET MVC versions `2012.2.710` through `2026.3.1015`, server-side filter processing does not properly validate descriptor types, null values, or stack state in FilterNodeVisitor and does not catch FilterParserException within the affected assembly. An unauthenticated remote attacker can exploit this if the application exposes an endpoint reachable without authentication that accepts crafted filter parameters. Affected requests can trigger uncaught cast, null-reference, or empty-stack exceptions and return HTTP 500. The report does not demonstrate worker-process termination or disruption of unrelated requests. The issue is fixed in version `2026.4.1111`.	8.6	More Details
CVE-2026-116059	The LetsRecover WordPress plugin through 1.2.0 does not sanitize a user-supplied value that is used as a database column name in one of its unauthenticated AJAX actions, allowing unauthenticated attackers to append SQL to the query and read arbitrary data from the database, which is then returned through a second unauthenticated action.	8.6	More Details
CVE-2026-	An authentication bypass using an alternate path or channel vulnerability in the rsync in Synology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1 allows remote	8.6	More Details

85101	attackers to read specific files, write arbitrary files, and conduct limited denial-of-service attacks.		
CVE-2026-106154	In Progress® Telerik® UI for ASP.NET Core versions `2015.1.318` through `2026.3.1015`, the server-side FilterParser processes nested expressions in untrusted filter parameters through recursive parsing without a recursion-depth limit, while FilterLexer does not enforce an input-length limit. An unauthenticated remote attacker can exploit this if the application exposes an endpoint using DataSourceRequest model binding that is reachable without authentication. Deeply nested filters can trigger parsing errors during model binding or cause `StackOverflowException`. This issue is fixed in version `2026.4.1111`.	8.6	More Details
CVE-2026-106137	In affected versions of Progress® Telerik® UI for ASP.NET MVC `2012.2.710` through `2026.3.811`, ClassFactory updates a shared class dictionary without exclusive write protection and emits non-collectible dynamic assemblies that remain loaded for the AppDomain's lifetime. The dictionary lookup and insertion are not atomic, and case variations in aggregate descriptors can produce distinct retained types even though member resolution is case-insensitive. An unauthenticated remote attacker can exploit this if the application exposes an aggregation endpoint that is reachable without authentication, by submitting concurrent or repeated crafted requests. These requests may corrupt dictionary state or increase CPU and memory use, potentially degrading availability. The issue is fixed in version `2026.3.1015`.	8.6	More Details
CVE-2026-106156	In Progress® Telerik® UI for ASP.NET Core versions `2015.1.318` through `2026.3.811`, repeated server-side aggregation requests, with or without grouping, cause dynamic assemblies and load contexts to be retained, resulting in accumulating process memory consumption. An unauthenticated remote attacker can exploit this if the application exposes an aggregation endpoint that is reachable without authentication. Repeated requests can cause memory growth that may exhaust available resources and affect application availability. Disabling grouping in the client-side interface does not prevent direct requests containing these descriptors. The issue is fixed in version `2026.3.1015`.	8.6	More Details
CVE-2026-111433	UNIX symbolic link (symlink) following vulnerability in openEuler iSulad on Linux. This vulnerability is associated with program file src/daemon/modules/spec/specs_mount.c. This issue affects iSulad: through 2.1.6. If an attacker can get the victim or the platform to run their crafted malicious image, they can cause the iSulad daemon to copy sensitive host directories into an anonymous volume when creating a container, which the container can then read.	8.6	More Details
CVE-2026-126238	A incorrect authorization vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to bypass authorization checks and gain unauthorized access to restricted functionality.	8.6	More Details
CVE-2024-58405	Zipline through 3.7.9 contains an improper authorization vulnerability in the /api/auth/register endpoint, which enforces invite codes only when user registration is disabled, so registration succeeds without an invite when both invites and user registration are enabled. Unauthenticated attackers can send a direct POST request omitting the invite code to create accounts, view stats, and exhaust storage by uploading many files.	8.6	More Details
CVE-2026-47711	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4, 1.5.1, and 1.6.0, the current master demo server can be crashed remotely over BACnet/IP by sending a valid Confirmed WriteProperty request that updates loop-1's controlled-variable-reference to point to life-safety-zone-1 / accepted-modes. This issue has been patched in versions 1.4.4, 1.5.1, and 1.6.0.	8.6	More Details
CVE-2026-58498	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, there is a remote global-buffer-overflow in the official router-ipv6 application shipped with bacnet-stack, this results in an out-of-bounds write to the global transmit buffer under ASan. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	8.6	More Details
CVE-2026-124265	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tribulant Software Newsletters newsletters-lite allows Blind SQL Injection.This issue affects Newsletters: from n/a through 4.18.1.	8.5	More Details
CVE-2026-125926	Server-side request forgery (SSRF) in the server registration and update API in Amazon mcp-gateway-registry before 1.35.0 might allow an authenticated remote user to send requests from the gateway to internal network services and cloud instance metadata endpoints and read the responses via a crafted request. To remediate this issue, users should upgrade to version 1.35.0.	8.5	More Details
CVE-2026-127214	Flowise through 3.1.4 contains a server-side request forgery vulnerability that allows authenticated attackers with chatflows or agentflows create/update permissions to bypass the Custom Function sandbox's SSRF protection by requiring a module subpath inside an allowlisted package, such as axios/dist/node/axios.cjs or node-fetch/lib/index.js, which evades the vm2 mock table and returns an unwrapped HTTP client that skips the checkDenyList validation. Attackers can issue arbitrary GET and POST requests with attacker-controlled bodies via POST /api/v1/node-custom-function to reach loopback and internal-network addresses or the cloud metadata endpoint, enabling network mapping, credential disclosure, and state changes on internal services.	8.5	More Details
CVE-2026-125832	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Passionate Programmer Peter WP Data Access wp-data-access allows SQL Injection.This issue affects WP Data Access: from n/a through 5.5.92.	8.5	More Details
CVE-2026-	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in myCred	8.5	More

125811	myCred mycred allows Blind SQL Injection.This issue affects myCred: from n/a through 4.0.2.		Details
CVE-2026-65952	Improper neutralization of special elements used in an OS command in the remote SSH operation functionality of Lenovo XClarity Essentials OneCLI 5.5.0 for Linux could allow an attacker to execute arbitrary OS commands with the privileges of the configured SSH account on a managed server by supplying a specially crafted remote path.	8.5	More Details
CVE-2026-123177	A flaw was found in dnf5daemon-server. Unauthenticated D-Bus methods pass caller-controlled URL or .rpm path patterns into a root-privileged cmdline package loader that may store fetched content in a world-readable cache without size limits, or open local paths as root, allowing a local attacker to disclose privileged content and to deny service via disk exhaustion.	8.4	More Details
CVE-2026-126180	A improper neutralization of special elements used in a template engine vulnerability in Fortinet FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2 all versions, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2 all versions may allow a low privileged Device Manager admin to obtain super admin privilege on managed FortiGates via injecting malicious commands.	8.4	More Details
CVE-2026-86355	Dell PowerStore contains an External Control of File Name or Path vulnerability. A remote authenticated attacker could exploit this vulnerability, potentially leading to privilege escalation on the appliance.	8.3	More Details
CVE-2026-126321	Dockhand before 1.0.55 contains a path traversal vulnerability that allows authenticated users with stacks:edit to bypass the file-browser path guard by combining symlinks with '..' sequences. Attackers can read /proc/self/environ, the SQLite database, and the encryption key via /api/system/files/content, or move them using the stack relocate endpoint, exposing stored credentials.	8.3	More Details
CVE-2026-126252	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an authenticated attacker to execute unauthorized code or commands via http requests	8.3	More Details
CVE-2026-67548	taOS is a self-hosted AI agent OS. Prior to version 1.0.0-beta.25, tinyagentos (taOS) registers all system settings routes under a single APIRouter() instance created with no admin authorization dependency. Any authenticated user—including non-admin invited users whose is_admin flag is explicitly False—can read the full system configuration, overwrite it, modify platform settings, trigger a git pull + dependency reinstall + service restart, and switch the tracked update branch. Successful exploitation of the write endpoints causes immediate configuration corruption or a denial of service for all users on the instance from a low-privileged account. This issue has been patched in version 1.0.0-beta.25.	8.3	More Details
CVE-2026-123638	The "Protected file patterns" setting of a branch protection rule was checked against file names as git prints them, and git quotes names that contain a double quote, a backslash or a control character. Such names never matched a pattern, so a user with write access could add or change files under a protected pattern by direct push or through a pull request merge, and could move a protected file out of the pattern's reach by renaming it. Where the patterns protect workflow files, this allowed adding a workflow that then ran on the repository's runners. Changed files are now listed unquoted, and a rename reports both the old and the new path.	8.3	More Details
CVE-2026-97039	Building a malicious package that uses "#cgo pkg-config:" directives could load untrusted pkg-config ".pc" files or inject unvalidated compiler and linker flags. The pkg-config flag allowlist previously permitted "--with-path=" and "--personality=", allowed "--define-variable=" values beginning with "=" or "$" (which can rewrite paths in system ".pc" files into sysroot-prefixed "-L=" or "-L$SYSROOT" linker search paths), and allowed package arguments ending in ".pc" or containing path separators or "..", which caused pkg-config to load local ".pc" files directly from the package directory. In addition, flags returned by "pkg-config --cflags" in cgoCPPFLAGS were not checked when determining whether internal linking is safe. The go command now disallows "--with-path=", "--personality=", leading "=" or "$" characters in "--define-variable=" values, and local ".pc" paths in "#cgo pkg-config:" directives, and inspects cgoCPPFLAGS when checking internal linking compatibility.	8.3	More Details
CVE-2026-129139	paicoding from commit b8206b9 through commit 903adce uses predictable credentials for accounts created via ZSXQ login, because loginByZsxq derives both the username and password solely from the member's ZSXQ number. Unauthenticated attackers can read that number from the victim's /user/{userId} profile page, compute the credentials, and log in via /login/username to take over the account.	8.2	More Details
CVE-2026-129261	A vulnerability was found in Kingston FURY CTRL RGB Control Software up to 2.0.66.0. The impacted element is an unknown function in the library NTIOLib_X64.sys of the component IOCTL Handler. Performing a manipulation results in exposed ioctl with insufficient access control. The attack is only possible with local access.	8.2	More Details
CVE-2026-126774	@tinacms/mdx before 2.4.2 contains a code injection vulnerability in its MDX serializer, which writes rich-text values into MDX expressions without escaping them. Authenticated content editors can save crafted values that break out of list field or highlightColor expressions in the stored .mdx file, executing JavaScript in visitors' browsers or on build and server-side rendering hosts.	8.2	More Details
	soapbar is a SOAP library for Python — client, server, and WSDL handling. Prior to version 0.13.0, verify_envelope_bsp() derived its trust anchor from the message it was verifying. It read the X.509 certificate out of the caller-untrusted wsse:BinarySecurityToken, validated only that certificate's not-before / not-after dates, and then verified the signature against that same certificate. There was no CA-chain validation, no issuer/subject		

CVE-2026-64855	allowlist, and no pinning. A successful verify_envelope_bsp() therefore proved only that the envelope was signed by whoever supplied the embedded certificate — never that it was signed by a trusted party. An attacker who mints their own certificate, signs a forged envelope, and embeds that certificate in the token passes verification. Any consumer that treats a successful BSP verification as authentication can be impersonated (signature forgery / authentication bypass). verify_envelope() (which pins a caller-supplied x509_cert) was not affected — the flaw was specific to the BSP variant whose trust anchor came from the message. This issue has been patched in version 0.13.0.	8.2	More Details
CVE-2026-126802	NextScan 1.1.0 through 1.2.0 contains hardcoded HTTP Basic Auth credentials in ns-admin's AuthAgent and AuthExternal routers that allow unauthenticated attackers to access protected APIs. Attackers can call /agent/config to obtain Redis passwords, etcd details and the server token, and impersonate scan nodes via registration, heartbeat and logging endpoints.	8.2	More Details
CVE-2026-45265	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4 and 1.5.1, there is a stack-based out-of-bounds write / stack-buffer-overflow in bacnet-stack when the server processes a malicious Atomic-Read-File request in record access mode. The bug is triggered on the real server side. A crafted request can set an excessively large RecordCount, which is later used as the loop bound for writing record data into a stack-allocated BACNET_ATOMIC_READ_FILE_DATA data structure. However, the stack object only has space for one fileData element. When the loop reaches i = 1, the code computes &data->fileData[1], which is already out of bounds, and the resulting invalid pointer is passed down to memmove(), causing a stack-buffer-overflow. This issue has been patched in versions 1.4.4 and 1.5.1.	8.2	More Details
CVE-2026-126383	n8n before 1.123.89, 2.x before 2.45.5, 2.46.x before 2.46.1, and 3.x before 3.0.1 contains a NoSQL injection vulnerability in the MongoDB node's Update and Find And Replace operations due to insufficient validation of the update key value taken from incoming items. Attackers who can supply untrusted input, such as a webhook body, to a workflow using these operations can make the node match and overwrite unintended documents or insert new documents in the MongoDB database.	8.2	More Details
CVE-2026-126218	A authorization bypass through user-controlled key vulnerability in Fortinet FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11 may allow a remote authenticated attacker with admin permission to elevate their privileges to root via crafted HTTP requests.	8.2	More Details
CVE-2026-124218	The Drag and Drop File Upload for Elementor Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the remove_files function in all versions up to, and including, 1.6.2 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). This vulnerability is reachable when the "yeepdf_not_save" privacy option is enabled, a commonly used production setting that triggers the remove_files() cleanup path.	8.2	More Details
CVE-2026-47710	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4, 1.5.1, and 1.6.0, a stack-buffer-overflow can be triggered in the current master branch when a Loop object reads a referenced property through its default timer path and the referenced property is OBJECT_STRUCTURED_VIEW / PROP_DESCRIPTION containing a long attacker-controlled string. This issue has been patched in versions 1.4.4, 1.5.1, and 1.6.0.	8.2	More Details
CVE-2026-126184	A authentication bypass by spoofing vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiAnalyzer-BigData 7.6.0 through 7.6.2, FortiAnalyzer-BigData 7.4.0 through 7.4.6, FortiAnalyzer-BigData 7.2.0 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an attacker to disrupt the HA state.	8.2	More Details
CVE-2026-47258	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4, 1.5.1, and 1.6.0, a stack-based out-of-bounds write exists in the Notification Class object implementation when handling AddListElement for the recipient-list property. This issue has been patched in versions 1.4.4, 1.5.1, and 1.6.0.	8.2	More Details
CVE-2026-126215	A incorrect authorization vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to escalate their privileges, bypass authorization controls or impersonate internal services via specially crafted requests to the GUI.	8.2	More Details
CVE-2026-126160	A improper authentication vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to escalate privileges and release or delete quarantined messages for arbitrary mailboxes via a crafted quarantine release requests.	8.2	More Details

CVE-2026-68905	Hugo Blog is a tech blog site. In commit 744ca15 and prior, the AI assistant proxy exposes three HTTP endpoints (POST /api/blog-assistant, POST /api/blog-search-embedding, POST /api/blog-search-rerank) without any authentication check. When deployed following the documented Nginx reverse-proxy setup, any unauthenticated remote attacker can send arbitrary requests that the proxy forwards to the upstream LLM/embedding/rerank API using the operator's server-side API key (OPENAI_API_KEY / AI_SEARCH_API_KEY). This enables unlimited quota consumption, cost exhaustion, and potential service unavailability for the operator. At time of publication, there are no publicly available patches.	8.2	More Details
CVE-2026-129445	A security flaw has been discovered in D-Link DIR-850L FW1.20WWb03. This impacts an unknown function of the file /usr/sbin/consolepwd of the component Console Login. Performing a manipulation results in hard-coded credentials. The attack requires a local approach. The exploit has been released to the public and may be used for attacks.	8.2	More Details
CVE-2026-126250	A incorrect authorization vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to cause a denial of service via HTTP requests.	8.2	More Details
CVE-2026-47259	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4, 1.5.1, and 1.6.0, a RemoveListElement request targeting Notification-Class.recipient-list can trigger a stack-based out-of-bounds write in the current master branch when the request contains more than NC_MAX_RECIPIENTS valid BACnetDestination elements. This issue has been patched in versions 1.4.4, 1.5.1, and 1.6.0.	8.2	More Details
CVE-2026-126240	A improper neutralization of special elements used in an ldap query ('ldap injection') vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an authenticated attacker to bypass authentication. Successful exploitation requires either a malicious/compromised upstream IdP, or an IdP configuration that allows the user to control the NameID (or the SAML attribute used as the username).	8.2	More Details
CVE-2026-111792	Uncontrolled Recursion vulnerability in Apache XML Graphics Batik. This issue affects Apache XML Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.	8.2	More Details
CVE-2026-124007	XWEB EVO before 5.6.2 contains a pre-authentication OS command injection vulnerability that allows unauthenticated remote attackers to execute arbitrary commands by injecting shell metacharacters into the password field. Attackers can exploit the unescaped interpolation of the password value into the hashpass invocation within login.lua, cleanout.lua, and api.lua to achieve root-level command execution via the setuid wlua interpreter. This product line reached it's end of service date in March 2026.	8.1	More Details
CVE-2026-126455	OpenEMR before 8.5.0 contains multiple missing authorization and SQL injection defects across report, portal, transaction, and immunization components. Low-privileged Front Office clerks can chain these to read arbitrary database tables including users_secure hashes, hijack patient portal identities, and forge approved clinical records.	8.1	More Details
CVE-2026-126480	OpenEMR before 8.5.0 contains an sql injection vulnerability in CcrTable::insertApprovedData() that allows authenticated users to inject SQL through request parameter names used as column names. Attackers can send crafted patient_data-*-sel parameters to the revandapprove route, lacking ACL and CSRF checks, to copy password hashes into patient fields or corrupt records.	8.1	More Details
CVE-2026-75864	Zohocorp ManageEngine DDI Central versions below 6301 is affected by an improper authorization vulnerability that allowed authenticated non-administrative users to delete DNS zones outside their assigned scope.	8.1	More Details
CVE-2026-124006	XWEB EVO through 5.8.8 contains a predictable credential generation vulnerability that allows attackers to derive the Linux root password by computing a fixed prefix combined with a daily password value. Attackers can calculate the deterministic root credential, which before 5.7.0 was identical across all units and from 5.7.0 onward remains derivable from the MAC-based daily password, to gain unauthorized root access to the underlying operating system. This product line reached it's end of service date in March 2026.	8.1	More Details
CVE-2026-119618	Concurrent Execution using Shared Resource with Improper Synchronization vulnerability in Apache HTTP Server's mod_http2 in assign_headers() can lead to RCE. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.70. Affected releases of mod_h2 from GitHub: from 2.0.8 through 2.0.42.	8.1	More Details
CVE-2026-126176	A xml injection (aka blind xpath injection) vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an unauthenticated remote attacker to inject arbitary content into a signed SAML response via crafted SAML requests.	8.1	More Details
	A xml injection (aka blind xpath injection) vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0,		

CVE-2026-126177	FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an unauthenticated remote attacker to inject arbitary content into a signed SAML response via crafted SAML requests.	8.1	More Details
CVE-2026-124005	XWEB EVO 4.3.0 through 5.8.8 contains a weak password generation vulnerability that allows remote attackers to derive the Administrator code-of-the-day password using only the device MAC address and date, with no server secret involved. Attackers can analyze the firmware binary xwpasswd, which itself functions as the password generator, to compute valid Administrator credentials offline and authenticate to the device without authorization. This product line reached it's end of service date in March 2026.	8.1	More Details
CVE-2026-126245	A out-of-bounds write vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to execute unauthorized code or commands via http requests, should the attacker be able to defeat ASLR protections.	8.1	More Details
CVE-2026-126442	OpenEMR before 8.5.0 contains a missing authorization vulnerability in create_portallogin.php that allows low-privilege authenticated users to replace patient portal credentials without ACL checks. Attackers can select a victim patient in session and post replacement credentials to take over portal accounts, read PHI, and lock patients out.	8.1	More Details
CVE-2026-115788	IBM App Connect Operator and IBM App Connect Enterprise Certified Containers Operands is vulnerable to Log Forging on a request to create a resource.	8.1	More Details
CVE-2026-126273	NocoDB before 2026.09.0 contains a privilege escalation vulnerability in initAdminFromEnv.ts that silently skips super-admin bootstrap when the admin password environment variable is empty. Unauthenticated attackers can call the public signup endpoint first on a fresh instance to receive Creator and Super Admin roles, gaining full administrative control.	8.1	More Details
CVE-2026-126375	Vvveb through 1.0.8.6 contains a missing authorization vulnerability that allows low-privilege vendors to rename, delete, or overwrite other vendors' digital-asset files in the shared storage/digital_assets directory. Attackers can send rename, delete, or upload requests to product/digital-asset with another vendor's filename to break downloads or substitute malicious content.	8.1	More Details
CVE-2026-75867	Zohocorp ManageEngine DDI Central versions below 6301 is affected by an authorization bypass vulnerability that allowed authenticated non-administrative users to modify Windows DHCP filter-list configurations across unauthorized clusters.	8.1	More Details
CVE-2026-75868	Zohocorp ManageEngine DDI Central versions below 6301 is affected by an authorization bypass vulnerability that allowed authenticated non-administrative users to modify DHCP options on subnets belonging to unauthorized clusters.	8.1	More Details
CVE-2026-14661	External control of file name in PostgreSQL dblink and CREATE/ALTER SUBSCRIPTION allows a user to achieve persistent denial of service, via appending invalid data to a chosen file. Specifically, the "sslkeylogfile" connection parameter appends data, in NSS keylog format, to a file of the user's choosing. This "sslkeylogfile" mechanism cannot add arbitrary bytes. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are also affected if libpq version 18 or later is installed and in use by the server.	8.1	More Details
CVE-2026-124012	XWEB EVO 5.6.2 through 5.8.8 contains a hardcoded credential vulnerability where the Administrator web account is configured to use password_mode daily_password with no stored password, as the Users.authenticate function in lualib_users.lua synthesizes the Administrator configuration without validating any stored secret. Attackers who can derive the MAC-based daily password can authenticate as Administrator to obtain a full admin session on the device. This product line reached it's end of service date in March 2026.	8.1	More Details
CVE-2026-111547	Dell PowerStore contains an out-of-bounds read vulnerability. An attacker could exploit this vulnerability, potentially leading to denial of service or limited information disclosure.	8.1	More Details
CVE-2026-127109	A code injection vulnerability in promzard’s template-loading functionality allows an attacker who can control property names in the context object (ctx) to execute arbitrary code with the privileges of the Node.js process. The library inserts context property names into a generated function’s parameter list without validation or escaping and evaluates the resulting source using `vm.runInThisContext()`. A crafted property name can escape the parameter list and inject JavaScript code, even when the template file is fully trusted.	8.1	More Details
CVE-2026-126720	Rooxis RXR-12 Wi-Fi router contains an unauthenticated remote code execution vulnerability in /usr/bin/cloud_manage, where a server-controlled JSON diagnoseParameter field is passed unsanitized to popen(), enabling arbitrary command execution as root over cleartext HTTP when an attacker is positioned on-path and has access to the hard-coded cloud endpoint. Firmware 20260813_c2169ea5 fixes the vulnerability, and your router can be updated through the local web interface.	8.1	More Details
CVE-2026-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes GrandPrix Core grandprix-core allows PHP Local File Inclusion.This issue affects	8.1	More

129091	GrandPrix Core: from n/a through 1.0.		Details
CVE-2026-121528	A improper certificate validation vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2.0 through 7.2.13, FortiOS 7.0 all versions, FortiOS 6.4 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the SSLVPN web portal and the backend destination website.	8.1	More Details
CVE-2026-126481	OpenEMR before 8.5.0 contains a path traversal vulnerability in era_payments.php and sl_eob_search.php that allows authenticated billing users to write files outside the ERA directory. Attackers can embed traversal sequences in the GS04 element of an uploaded X12 835 file to overwrite .edi or .835 files with attacker-controlled content anywhere writable by the web server.	8.1	More Details
CVE-2026-109870	The User Registration & Membership WordPress plugin before 5.3.2 does not verify that a discount coupon applied to a paid membership plan is actually valid for that plan before treating a fully discounted order as paid, allowing unauthenticated users to be granted the role mapped to a paid plan without paying for it, which can lead to privilege escalation up to administrator where a plan is mapped to a privileged role.	8.1	More Details
CVE-2026-67541	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.70, team-member management (add / remove / update) is gated only on team membership, not on the team creator/admin role — and TeamMember has no role column. Any non-creator member can seat an attacker account into the team; because credential team-shares are scoped only by TeamMember.user_id, the newly-added attacker can then decrypt every credential shared into that team (provider API keys, OAuth tokens. This issue has been patched in version 0.0.70.	8.1	More Details
CVE-2026-126163	A use of externally-controlled format string vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1 may allow a remote unauthenticated attacker to execute unauthorized code or commands via a specially crafted SMTP command.	8.1	More Details
CVE-2026-110279	IBM ContextForge MCP Gateway 1.0.0 through 1.1.0 is vulnerable to improper credential handling because the X-Upstream-Authorization request header can override the gateway-managed upstream credential for OAuth (authorization_code and client_credentials), bearer and basic authenticated gateways, which could allow an authenticated user to cause upstream requests to be made with a different credential and bypass per-user permission and audit attribution.	8.1	More Details
CVE-2026-47257	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. In versions 1.5.0 and 1.6.0-rc1, there is a restore logic flaw in bacnet-stack that is reachable through the official, unmodified apps/server management path when BACNET_BACKUP_RESTORE is enabled. This issue has been patched in versions 1.5.1 and 1.6.0.	8.1	More Details
CVE-2026-126804	WWBN AVideo 12.4 through 29.7.1 contains a path traversal vulnerability in the ADs plugin deleteImage.json.php that allows authenticated users with custom ads to delete arbitrary files. Attackers can set the unvalidated is_regular_user parameter to another user's id or ../ sequences to delete other users' ads or files like videos/configuration.php, taking the site offline and re-exposing the installer.	8.1	More Details
CVE-2026-102612	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.6, 1.5.2, and 1.6.1, bws_srv_start() in ports/linux/websocket-srv.c builds the libwebsockets server context with a CA certificate loaded but never sets LWS_SERVER_OPTION_REQUIRE_VALID_OPENSSL_CLIENT_CERT, so the hub accepts TLS connections from clients presenting no certificate at all. Any network-reachable host can join the BACnet/SC mesh without credentials. This issue has been patched in versions 1.4.6, 1.5.2, 1.6.1, and 1.7.0.	8.1	More Details
CVE-2026-75495	Cudy TR3000 before 2.5.42 contains an OS command injection vulnerability that allows a malicious or compromised ACS to execute commands as root by supplying a crafted InternetGatewayDevice.User.{i}.Password value. Attackers can send a SetParameterValues request with shell metacharacters that obuspa_system.lua concatenates into a luci.util.exec() command string, gaining root command execution.	8.1	More Details
CVE-2026-19048	An improper link resolution before file access vulnerability in the thumb in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write arbitrary files and conduct denial-of-service attacks.	8.1	More Details
CVE-2026-18596	An authentication bypass using an alternate path or channel vulnerability in the OTP in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers with valid user credentials to read or write arbitrary files and conduct denial-of-service attacks.	8.1	More Details
CVE-2026-129167	Seafile SeaDoc converter 2.0.4 before 2.0.11 and 3.0.0 before 3.0.8 contains an absolute path traversal vulnerability that allows unauthenticated attackers holding a public share token to execute code. Attackers supply an absolute filename to /api/v1/confluence-to-wiki/ to extract a ZIP from download_url into the Python library path, then trigger the module's import via a file-convert request.	8.1	More Details
CVE-2026-126896	Missing authorization in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-	The WPCOM Member WordPress plugin before 1.8.3 does not limit or bind attempts to verify WeChat login codes, allowing unauthenticated attackers to brute-force a code issued to another user and log in as that user, including	8.1	More

123711	administrators, when WeChat official-account keyword login is enabled.		Details
CVE-2026-124496	The DRPC HTTP endpoint lets an authenticated client act as another user without applying the configured impersonation authorizer. An authenticated user can execute DRPC functions that are restricted to another user. Users are recommended to upgrade to version 3.2.0, which fixes the issue.	8.1	More Details
CVE-2026-126430	OpenEMR before 8.5.0 contains an sql injection vulnerability that allows any authenticated core user to inject SQL by supplying crafted patient_data field names to the CCR revandapprove controller. Attackers can embed scalar subqueries in the UPDATE patient_data SET clause to read staff password hashes and portal reset values, alter arbitrary patient demographics, and take over patient-portal accounts.	8.1	More Details
CVE-2026-126952	Zipline through 4.4.0 contains an authentication bypass vulnerability in the WebAuthn login endpoint that creates sessions for a supplied registered credential ID without verifying the assertion. Attackers who obtain a target's passkey credential ID can impersonate that account without its authenticator, potentially gaining administrative control over SUPERADMIN accounts.	8.1	More Details
CVE-2026-126903	Improper state validation in ANGLE in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-126953	Cudy TR3000 before 2.5.42 contains an OS command injection vulnerability that allows a malicious or compromised ACS to execute commands as root by supplying an unvalidated InternetGatewayDevice.User.{i}.Username value. Attackers can send a SetParameterValues request with shell metacharacters that set_UserUsername() in obuspa_system.lua passes to os.execute(), gaining root command execution.	8.1	More Details
CVE-2026-63150	Omnispace Agora Project through 26.10.0 contains a cross-site request forgery vulnerability that allows remote attackers to forge privileged actions such as administrator user creation by merging $_GET and $_POST parameters without requiring an anti-CSRF token. Attackers can craft a malicious link or auto-navigating page that issues a plain GET request, exploiting the lack of CSRF protection and SameSite=Lax cookie behavior on top-level navigations to create unauthorized administrator accounts.	8.1	More Details
CVE-2026-126539	Directus before 12.1.0 contains an authorization bypass vulnerability that allows unauthenticated attackers to skip permission checks by sending a failed auth message on public-mode WebSocket connections. Attackers can send an invalid token so handleAuthRequest sets accountability to null, then read, create, update or delete records in any user-defined collection.	8.1	More Details
CVE-2026-129134	MRBS before 1.13.0 contains a password reset poisoning vulnerability that allows unauthenticated attackers to redirect reset links by forging the Host header when $url_base is unset. Attackers can request a reset for a victim so AuthDb::notifyUser() emails a link pointing to their host, capturing the reset key when opened to take over accounts including administrators.	8.1	More Details
CVE-2026-126377	Vvveb before 1.0.9.0 contains an authentication bypass vulnerability in generateCookie() in system/user/user.php that uses loose comparison to validate MD5 cookie hashes. Unauthenticated attackers can brute-force cookie values until the server's MD5 computation yields a 0e magic hash, then forge persistent cookies for account takeover.	8.1	More Details
CVE-2026-126196	pgEdge Postgres MCP Server enables SQL queries against PostgreSQL databases through Model Context Protocol compatible clients. Prior to 1.1.0, query_database on a read_only connection could send unrecognized statements through pgx Exec without bind parameters, selecting PostgreSQL's simple query protocol and allowing multiple semicolon-separated statements in one request. A caller could combine transaction or session state changes with database writes, and pooled session state could leave later calls writable, when the connecting role held write privileges. The flaw affected deployments relying on read_only as a safety boundary, could compromise integrity and availability, and did not add confidentiality impact beyond the reads already permitted by the connection. This issue is fixed in 1.1.0.	8.1	More Details
CVE-2026-119258	The Swipe WordPress plugin through 1.4 does not properly authenticate a login request before issuing a WordPress session cookie, allowing unauthenticated attackers to log in as an existing user, including an administrator, when that user has an active app session.	8.1	More Details
CVE-2026-118191	The Photo Gallery, Sliders, Proofing and Themes – NextGEN Gallery plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the handle_job function in all versions up to, and including, 4.5.5 This makes it possible for authenticated attackers, with custom-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). The 'NextGEN Manage gallery' capability required to reach the vulnerable endpoint is granted to Administrators by default but can be delegated to lower-privileged roles via the plugin's Roles screen.	8.1	More Details
CVE-2026-129126	C-Kermit before 11.1.515 contains a heap buffer overflow vulnerability in putsrv() in ckcfns.c that allows malicious peers to write past the srvcmd buffer by sending crafted packets. Attackers can use Kermit repeat-count compression in server command, GET, or file-header packets to write attacker-chosen bytes beyond the heap buffer on servers or receiving instances.	8.1	More Details
CVE-2026-129125	C-Kermit 6.0.192 before 11.1.515 contains a remote code execution vulnerability that allows Kermit clients to run shell commands on servers with host commands disabled by abusing REMOTE QUERY evaluation. Attackers can send a REMOTE QUERY invoking the command function, or define a macro via REMOTE ASSIGN and call	8.1	More Details

	execute to reach RUN, bypassing the nopush restriction and DISABLE HOST.		
CVE-2026-129124	C-Kermit before 11.1.515 contains an OS command injection vulnerability that allows remote clients to execute shell commands by supplying unquoted arguments to REMOTE WHO or REMOTE SPACE. Attackers can append shell metacharacters to arguments passed through WHOCMD or SPACM2 to syscmd(), executing commands on the server host even when DISABLE HOST is set.	8.1	More Details
CVE-2026-116417	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains a Weak Password Requirements vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Information disclosure and Unauthorized access.	8.1	More Details
CVE-2026-127215	Kanbanz by Softaculous plugin for WordPress before 1.0.3 contains a broken access control vulnerability that allows authenticated Kanban Staff users to access and modify boards they are not members of by exploiting admin-ajax handlers that fail to call kanbanz_user_can_access_board() or per-task edit checks on attacker-supplied board_id or task_id parameters. Attackers can supply arbitrary board IDs to read sensitive task data, overwrite status columns, subtasks, and labels, inject comments, upload or delete attachments, and create tasks or set WIP limits on boards owned by other teams.	8.1	More Details
CVE-2025-71459	Zipline through 4.3.2 contains a path traversal vulnerability that allows authenticated uploaders to write files outside the upload directory by supplying traversal sequences in the x-zipline-filename header. Attackers using the local datasource can create or overwrite files writable by the Zipline process, corrupting application data or disrupting service.	8.1	More Details
CVE-2026-127088	2FAuth before 9.0.1 contains a weak password recovery vulnerability that allows unauthenticated attackers to poison reset links by forging the HTTP Host header. Attackers can request password or WebAuthn recovery emails with an attacker-controlled host, capture the victim's token, and take over accounts exposing stored TOTP/HOTP secrets.	8.1	More Details
CVE-2026-126454	OpenEMR before 8.5.0 lacks rate limiting or lockout on TOTP submission, allowing attackers with a valid password to brute-force the 6-digit MFA code. Attackers can script repeated POST requests to main_screen.php or the OAuth2 authorization flow with re-submitted hidden credentials to bypass two-factor authentication.	8.1	More Details
CVE-2026-124020	Control Web Panel (CWP) before webpanel_version 1.30.6 contains a host header injection vulnerability that allows unauthenticated attackers to manipulate the password-recovery reset URL by injecting the HTTP Host header into the /v1/lostpass/ route's token generation process. Attackers can lure an automated mail-security scanner into visiting the poisoned reset link to exfiltrate the live recovery token, replay it at /login/index.php?acc=newpass to set a new password, and subsequently abuse the File Manager and Crontab modules to achieve command execution as the targeted hosting account.	8.1	More Details
CVE-2026-111579	The Forminator Forms WordPress plugin before 1.58.4 does not enforce payment on the server side when a form's configured payment gateway is unavailable, allowing unauthenticated visitors to complete a payment-gated User Registration form without paying and be assigned the form's configured role, up to administrator, after the gateway has been connected and later disconnected.	8.1	More Details
CVE-2026-81584	An improper neutralization of special elements used in an SQL command vulnerability in the User API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers with control over a compromised LDAP or Active Directory server to read or write arbitrary files and conduct denial-of-service attacks.	8.1	More Details
CVE-2026-71531	PrestaShop before 8.2.9 and 9.2.1 contains an authorization flaw in the Webservice API that allows an attacker holding a key restricted to one shop to act on data of every shop by submitting requests with id_shop=all or id_shop_group=N, which expand the shop context without validating the key's actual shop associations and cause shopHasRight() to evaluate the expanded set as a disjunction. Attackers can exploit this flaw via classes/webservice/WebserviceRequest.php to read, modify, or delete data belonging to shops they are not authorized for, including full customer records such as email addresses, secure_key, and password hashes across the installation.	8.1	More Details
CVE-2026-111190	The ARForms plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 7.2.4 via its form file-upload handler. The name of the stored file is taken from an attacker-controlled request header and is not adequately restricted to safe file types, and the plugin's file-type and content-safety checks can be evaded, allowing files that contain executable PHP code to be written to a publicly accessible directory. This makes it possible for unauthenticated attackers to upload malicious files to the affected site's server, which may make remote code execution possible. Exploitation requires a published form containing a File field to be publicly accessible on the site.	8.1	More Details
CVE-2026-124021	Control Web Panel (CWP) before webpanel_version 1.30.6 contains an authorization bypass vulnerability in the validate() function of api/v1/index.php that allows attackers holding a password-recovery token and a predictable legacy signature to obtain valid remote-API authorization without a proper API key. Attackers can exploit this flaw via the POST /cronjobsusers/ endpoint to add arbitrary cron commands and achieve command execution as the affected hosting account, and can also abuse the same token to access global account-list and account-detail routes exposing usernames, contact emails, and password hashes.	8.1	More Details
	node-fontnik is a library that delivers a range of glyphs rendered as SDFs (signed distance fields) in a protocol buffer. Prior to version 0.7.7, a crafted font could trigger a heap out-of-bounds write in RenderSDF		

CVE-2026-63660	(include/mapbox/glyph_foundry_impl.hpp). RenderSDF computed the SDF bitmap allocation size as buffered_width * buffered_height in 32-bit unsigned int. Glyph dimensions are derived from the uploaded font's outline bounding box with no upper bound, so a glyph large enough to make that product exceed 2^{32} wrapped to a small value. The buffer was then under-allocated while the render loop still wrote one byte per pixel, corrupting the heap (CWE-190 → CWE-787) and crashing the process. A 680-byte font is enough to drive FreeType to a 65536×65536 buffered glyph, wrapping the size to 0. This issue has been patched in version 0.7.7.	8.1	More Details
CVE-2026-120148	Type confusion in PostgreSQL extended statistics allows an object creator to execute arbitrary code as the operating system user running the database, via a statistics expression of an anonymous RECORD type whose backend-local type identifier denotes a different row type in another session. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	8.1	More Details
CVE-2026-126286	NocoDB before 2026.08.0 contains a reflected cross-site scripting vulnerability in PageLeavingWarning.vue that allows unauthenticated attackers to execute script by embedding an ASCII control character in the ncRedirectUrl scheme. Attackers can send a crafted link that bypasses the scheme check and reaches the anchor href or window.location, stealing the session token from localStorage for account takeover.	8.1	More Details
CVE-2026-126322	OpenEMR before 8.3.0 contains an unsanitized deserialization vulnerability that allows authenticated attackers to control patient-matching criteria by supplying a crafted serialized key parameter. Attackers can send serialized arrays to interface/orders/patient_match_dialog.php to enumerate patients or force matches that associate lab orders with the wrong patient.	8.1	More Details
CVE-2026-126434	OpenEMR before 8.5.0 contains a missing authorization vulnerability in interface/forms/procedure_order/common.php that allows authenticated accounts lacking patients/lab permission to read and modify other patients' procedure orders. Attackers can request a global order id to disclose clinical history, or select the target patient in their session and submit bn_save to falsify diagnoses, instructions, and order status.	8.1	More Details
CVE-2026-71519	PrestaShop before 8.2.9 and 9.2.1 contains a broken access control vulnerability that allows an authenticated Webservice API key holder to read and modify customer records belonging to any shop in a multi-shop installation. Attackers can exploit the missing record-level shop ownership check in shopHasRight() and saveEntityFromXml() to read sensitive customer data such as password hashes and secure keys, and change a customer's email and password via create, update, and delete requests, resulting in account takeover.	8.1	More Details
CVE-2026-91869	IBM Security QRadar EDR 3.12 through 3.12.26 could allow a remote authenticated attacker to bypass security restrictions due to improper rate limiting on TOTP verification.	8.1	More Details
CVE-2026-126541	WWBN AVideo through 29.7.1 contains a missing authorization vulnerability in Live plugin restream endpoints that allows authenticated streamers to obtain other users' stream keys by supplying arbitrary live_transmitions_history_id values. Attackers can redeem the issued action tokens at verifyTokenForAction.json.php to retrieve victims' HLS URLs and stream keys, then publish as the victim or restream private or pay-per-view lives.	8.1	More Details
CVE-2026-126875	Missing authorization in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-128047	OpenMage magento-lts before 20.18.2 and 21.0.0-beta pre-releases before 21.0.0-beta3 generate customer email-confirmation keys with md5(uniqid()) and customer and administrator password-reset tokens with the non-cryptographic uniqHash(). Unauthenticated attackers can brute-force the roughly 20-bit confirmation key via the unrate-limited confirmAction endpoint to log in as pending customers, or predict administrator reset tokens after recovering generator state.	8.1	More Details
CVE-2026-128014	FrankenPHP standalone static binaries 1.8.0 before 1.13.2 bundle the PHP brotli extension statically linked with Brotli 1.2.0, whose decoder contains an out-of-bounds write (CVE-2026-111497). Unauthenticated remote attackers can send crafted data to applications that pass it to brotli_uncompress_add() to crash the entire FrankenPHP process, and possibly cause memory disclosure or code execution.	8.1	More Details
CVE-2026-128046	OpenMage magento-lts 20.17.0 before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains an unrestricted file upload vulnerability because the general/file/protected_extensions blocklist omits phar, php8, and phps. Unauthenticated attackers can upload a .phar file through a product File custom option to a predictable media/custom_options path and request it directly to execute code on servers that map .phar to PHP and serve that directory.	8.1	More Details
CVE-2026-126937	Zipline before 4.6.5 contains a TOCTOU race condition in the POST /api/setup endpoint that allows unauthenticated attackers to create multiple SUPERADMIN accounts by racing concurrent requests before the firstSetup flag is reset. Attackers can send simultaneous requests with spoofed X-Forwarded-For headers during the argon2 hashing window to gain full administrative control of the instance.	8.1	More Details
CVE-2026-	Cudy TR3000 before 2.5.42 contains an authentication bypass vulnerability in the Mosquitto plugin auth_plugin_jwt.so that accepts unsigned JWTs using alg none. Attackers holding any Cudy-trusted client	8.1	More

75491	certificate can authenticate as admincudydevice on port 8883 and publish batchcmd requests to execute commands as root.		Details
CVE-2026-76792	The User Verification by PickPlugins WordPress plugin before 2.0.49 does not rate limit the verification step of its one-time-password login, and does not expire the generated code, allowing unauthenticated attackers to brute force it and log in as any user, including administrators, where the code is configured to use digits only.	8.1	More Details
CVE-2026-126815	Pre-account hijacking in the authentication flow in Lagarto Chivato 0.4.1 and earlier on Web allows remote unauthenticated attackers to take over arbitrary accounts via a password planted on an unregistered email address that becomes valid upon the victim’s first passwordless login.	8.1	More Details
CVE-2026-126282	NocoDB from 2026.04.0 before 2026.08.0 contains an improper privilege management vulnerability in org-users.service.ts where updating a user's legacy organization role rewrites their default-workspace role. Revoked users can silently regain Creator-level read, write and schema modification access across all default-workspace bases using their existing session token.	8.0	More Details
CVE-2026-126306	EspoCRM before 9.3.11 and 10.x before 10.0.8 contains a stored cross-site scripting vulnerability that allows low-privileged users to upload crafted SVG images that submit authenticated POST requests to arbitrary backend endpoints. Attackers can trick an administrator into opening the SVG in a separate browser tab and clicking it, performing administrator actions such as elevating the attacker's account to administrator.	8.0	More Details
CVE-2026-128041	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 serves RSS feeds with a text/html content type and does not escape feed entry data, leading to stored cross-site scripting. An unauthenticated guest can submit a product review with script in the nickname, title or text that executes when an administrator opens the pending-reviews feed, enabling admin account takeover.	8.0	More Details
CVE-2026-126793	An untrusted search path issue in Aurora PostgreSQL dialect detection in the AWS Advanced Go Wrapper from release 2026-04-06 (awssql/v2.0.0) and before release 2026-07-29 (awssql/v2.0.3) could allow a remote authenticated user to escalate privileges to those of another database user, including a member of the rds_superuser role, via a crafted function that runs when that user connects to an Aurora PostgreSQL cluster through an affected version of the wrapper. To remediate this issue, users should upgrade to the AWS Advanced Go Wrapper release 2026-07-29 (awssql/v2.0.3) or later.	8.0	More Details
CVE-2026-126181	A use of hard-coded credentials vulnerability in Fortinet FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11 may allow an adjacent-network authenticated attacker with user permission to join the FGFM configuration-sync mesh of the affected FortiGate deployment via the default pre-shared key.	8.0	More Details
CVE-2026-116325	SQL injection in PostgreSQL reindexdb allows an object creator to execute arbitrary SQL as the database user running reindexdb, via a crafted index name embedded in the parallel catalog query for --jobs with --index. Within major versions 17-18, minor versions before PostgreSQL 18.7 and 17.12 are affected. Versions before PostgreSQL 17 are unaffected.	8.0	More Details
CVE-2026-121876	A flaw was found in the interaction between systemd-gpt-auto-generator and confidential computing guest VM images in OpenShift Sandboxed Containers (confidential peer pods). systemd-gpt-auto-generator automatically discovers and mounts GPT partitions by type GUID at boot with no user confirmation. In the confidential computing threat model, where the host/hypervisor is the adversary, a malicious host can inject partitions into the guest's virtual disk. Most critically, injecting a swap partition causes the guest kernel to page out TEE-encrypted memory to a host-controlled block device, breaking the confidentiality guarantee of the hardware TEE (AMD SEV-SNP, Intel TDX). The PodVM images use a GPT-partitioned disk with dm-verity on the root partition. However, the roothash= kernel parameter only disables root auto-discovery — non-root partitions (swap, /home, /var, /srv, /var/tmp) are still auto-discovered and mounted. The generator is shipped unmasked in the RHEL systemd-udev subpackage, and no kernel command line parameter in the measured UKI addon disables it. Additionally, the PodVM measurement script captures PCRs 3, 9, 11, and 12, but not PCR 5 (GPT partition table), so partition table modifications are not detected by remote attestation.	7.9	More Details
CVE-2026-126497	LibreCAD through 2.2.1.6 contains a heap-based out-of-bounds write vulnerability in the bundled libdxfrw dwgReader18::parseDataPage() function due to unchecked buffer size and page offsets. Attackers can craft an AC1018 (R2004) DWG file with malicious startOffset values that cause decompress18 to write past the heap buffer when opened, causing crashes and potential code execution.	7.8	More Details
CVE-2026-109091	A buffer overflow in handling EDID Display-Range descriptors in X.Org xwayland before 24.1.15 and X Server before 21.1.26 could be used by malicious monitors to crash the x server or execute cote.	7.8	More Details
CVE-2026-108472	A flaw was found in the xfs_admin utility in xfsprogs. The tool does not properly validate user-supplied parameters, allowing operating system command injection. A local attacker can exploit this issue by providing crafted input arguments, which may result in arbitrary command execution and local privilege escalation depending on how xfs_admin is executed.	7.8	More Details
CVE-2026-15465	Software installed and run as a non-privileged user may conduct improper GPU system calls through the DDK kernel module interface. Under unsupported use of the interface, a use-after-free condition may occur that can lead to kernel memory corruption, platform instability, or system reboot. The weakness occurs when software references memory after it has been released. Accessing memory after free may result in corruption of valid	7.8	More Details

	data structures, unexpected program behaviour, process crashes, or execution of unintended operations.		
CVE-2026-92083	Missing Authorization vulnerability in TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü pardus-image-writer allows Privilege Escalation. This issue affects pardus-image-writer: before 0.9.0.	7.8	More Details
CVE-2026-18767	A local low privileged attacker or process can access I/O ports via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.	7.8	More Details
CVE-2026-124699	In Telerik UI for WinForms, versions prior to 2026.4.1111, an improper control of code generation vulnerability exists that allows an attacker to supply a crafted expression and execute unauthorized code in the context of the affected application.	7.8	More Details
CVE-2026-126607	Progressive Robot hMailServer 6.2.3 through 6.3.7 on Windows, with a MySQL or MariaDB database, hands the bundled MariaDB Connector/C the folder of its authentication plugins (the plugin folder in the installation's Bin folder) as Latin-1 bytes, which the client reads in the system's ANSI code page when it builds a plugin's path and loads the plugin with LoadLibraryExA, which allows a local authenticated user to execute code as the hMailServer service's account (LocalSystem, or the service's virtual account for a new installation from 6.3.4) by creating the folder those bytes name in the code page and placing in it a DLL with a plugin's name, when the installation folder's path holds a character between U+0080 and U+00FF whose byte the code page reads as another character, and none above U+00FF, and the user can create that other folder (by default any authenticated user may create a folder directly under the root of the system drive). The server converted the path with the C runtime's wcstombs_s in the C locale, which writes each character up to U+00FF as the byte of the same value: on code page 1252 those bytes are the same letters, while on another code page, such as 1251, or on a UTF-8 code page, they name another folder. The client loads the plugin the database server names in its greeting, unless it is built in, and any plugin the server names in an authentication switch, and tries again at each connection while a load fails, so with a MySQL 8.0 or later server, whose greeting names caching_sha2_password by default, the DLL is loaded at the next connection the service makes, whatever plugin the database account uses; a DLL's entry point runs when it is loaded. A path holding any character above U+00FF was handed over as an empty string, whatever the code page, from which the client makes a plugin's name at the root of the current drive: for the service, whose current folder is System32, that is the root of the system drive, where by default only administrators can create a file, but the server's own database commands (hMailServer.exe --check-database, --upgrade-database and the others from 6.3.4, and the /Debug and /Test console modes from 6.2.3) run in the folder they are started from - the product tells administrators to run them from an elevated prompt in the Bin folder, and the setup of 6.3.4 and 6.3.5 ran two or three of them itself with the Bin folder as their working folder for a new installation with an external database - so a DLL that a local authenticated user placed under a plugin's name at the root of a drive other users may write, such as a FAT or exFAT volume, was loaded into the administrator's process at the command's first connection to a MySQL 8.0 or later server. 6.3.8 fixes both cases: it hands the folder in the code page's bytes or by its short (8.3) name, and where neither can be written, a folder under the Windows system folder that holds no plugin and that only administrators can create, or else refuses the connection before attempting it; it never hands the empty value or a folder the current drive completes. The configuration is not the default: the default installation folder, under Program Files, is ASCII. Linux builds set no plugin folder and are not affected.	7.8	More Details
CVE-2026-128134	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. Prior to 3.10.4, nltk.parse.dependencygraph.dot2img resolves the Graphviz dot executable through PATH but invokes the resulting absolute executable without routing through spawn_trusted, so resolve_trusted_executable ownership and writability validation and safe_env loader environment scrubbing do not run. A local low-privileged attacker who can write to a directory on a POSIX victim's PATH can plant or replace dot, and code executes as the victim when dot2img is called directly or DependencyGraph.repr_svg renders a graph. The current-working-directory-only bare-name vector is blocked and is not this vulnerability; this issue is the residual writable absolute PATH element bypass after CVE-2026-78680. This issue is fixed in version 3.10.4.	7.8	More Details
CVE-2026-126612	Improper link resolution in the Windows installer of Progressive Robot hMailServer 6.0.0 through 6.3.7 allows a local authenticated user to run code as the mail server's service account or as an administrator when the path to the program folder passes through a junction, a symbolic link or a mount point that the user controls or that every user may change, such as a junction made at the root of a drive, which takes the root's permissions, or through a folder that every user may rename. Setup installed the programs through any such link without first checking who controls it, or whether a folder above the program folder may be renamed, and the service is registered to run the programs by that path, so the programs are installed where a link another account controls leads, or that account can later make the path lead to a folder it controls; the service, which runs as LocalSystem or as its virtual account, and the programs administrators run from Bin are then started from there. 6.3.7's fix for CVE-2026-107571 does not cover this: its hardening of the program folder, Bin and ControlPanel does not change a folder reached through a link that the administrators do not alone control, and setup does not refuse such a path: it installs through the link and at most reports afterwards that the folders could not be hardened. The default installation under Program Files is not affected.	7.8	More Details
CVE-2026-123040	An attacker who gains the ability to execute arbitrary code on a system with TrueConf Server (Linux) versions from 4.7.2 up to, but not including, 5.5.6 installed, running as the user trueconf (by exploiting some other vulnerability), can elevate their privileges to root.	7.8	More Details

CVE-2026-87772	Incorrect Authorization vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute Pardus About allows Privilege Escalation. This issue affects Pardus About: before 1.2.5.	7.8	More Details
CVE-2026-18768	A local low privileged attacker can access arbitrary physical memory or define its mapping via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.	7.8	More Details
CVE-2026-102632	Incorrect privilege assignment in the app token management component in Devolutions PowerShell Universal 2026.3.4 and earlier allows an authenticated user with token creation or update permissions to escalate privileges to administrator, and allows a revoked app token to be reinstated in multi-node deployments, via crafted app token requests that set an arbitrary role or revocation state.	7.8	More Details
CVE-2026-18769	A local low privileged attacker can move arbitrary physical memory content via TcRouter.sys because of exposed IOCTL function calls resulting in a full compromise of the affected devices.	7.8	More Details
CVE-2026-109903	A buffer overread caused by casting a negative integer to CARD32 in XvQueryImageAttributes in X.Org X Server before 21.1.26 and xwayland before 24.1.15 could be used to causes crashes by authenticated X clients.	7.8	More Details
CVE-2026-124700	In Telerik UI for WinForms, versions prior to 2026.4.1111, an untrusted URL redirection vulnerability exists that allows an attacker to launch arbitrary operating system protocol handlers with attacker-controlled arguments via crafted documents and hyperlinks with a non-allowlisted URI scheme that the user opens.	7.8	More Details
CVE-2026-124702	In Telerik UI for WPF, versions prior to 2026.4.1110, an untrusted URL redirection vulnerability exists that allows an attacker to launch arbitrary operating system protocol handlers with attacker-controlled arguments via crafted documents and hyperlinks with a non-allowlisted URI scheme that the user opens.	7.8	More Details
CVE-2026-128990	xschem 2.9.9 through 3.4.7 contains a heap out-of-bounds write vulnerability in read_dataset() in src/rawtovcd.c due to an unchecked variable index. Attackers can supply a crafted ngspice .raw file that, when converted with rawtovcd, writes file-controlled heap pointers at chosen signed offsets, corrupting heap memory.	7.8	More Details
CVE-2026-129128	Goose CLI 1.35.0 before 1.53.0 contains a local code execution vulnerability that allows attackers to run commands by setting diff.external in a repository's .git/config. Attackers can ship a crafted repository that, when the victim runs goose review, executes git diff without --no-ext-diff, running commands as the user and exposing credentials and provider API keys.	7.8	More Details
CVE-2026-89061	During an internal security assessment, a potential vulnerability was discovered in Lenovo PC Manager, distributed exclusively in the Chinese market, that could allow a local user to escalate privileges.	7.8	More Details
CVE-2026-129137	Incorrect default permissions in the agent configuration folder in Devolutions PowerShell Universal 2026.3.4 and earlier allows a local unprivileged user to execute arbitrary code as SYSTEM via a crafted agent configuration file that points the agent to an attacker-controlled server.	7.8	More Details
CVE-2026-124701	In Telerik UI for WinForms, versions prior to 2026.4.1111, a deserialization of untrusted data vulnerability exists that allows an attacker to perform unauthorized actions in the context of the affected application.	7.8	More Details
CVE-2026-124703	In Telerik UI for WPF, versions prior to 2026.4.1110, an improper control of code generation vulnerability exists that allows an attacker to execute unauthorized code in the context of the affected application.	7.8	More Details
CVE-2026-77882	A deserialization of untrusted data vulnerability was discovered in Lenovo System Update that could allow a local authenticated user to execute code with elevated privileges.	7.8	More Details
CVE-2026-126724	Rooxis RXR-12 Wi-Fi router contains an undocumented UID-0 backdoor account (dg) with a firmware-wide default password (ivanlee) and interactive shell (/bin/ash), allowing authentication as root via SSH or local console without device-specific secrets. Firmware 20260813_c2169ea5 removes the account from the shipped root filesystem and disables root password authentication in SSH. Users can update their router can be through the local web interface.	7.8	More Details
CVE-2026-123039	The Gaia OS DynamicCLI daemon runs as root and listens on a world-writable local socket (/tmp/dynamic_socket) without authenticating connecting processes. An authenticated local user can send a command to the socket and have it executed as root.	7.8	More Details
CVE-2026-110331	A flaw was found in abrt. The completeness check introduced to mitigate CVE-2026-54228 and CVE-2026-54229 only verifies that a dump directory contains a "count" element, which an unprivileged user can create. This allows a local attacker to bypass the guard and again poison elements in, or seize ownership of, dump directories while privileged ABRT handlers are processing them. Related Problems2 mutating methods remain ungated by the same check.	7.8	More Details
CVE-	Incorrectly handled negative sizes when processing ProcXvShmPutImage requests in the X.Org xwayland before		

2026-109092	24.1.15 and X Server before 21.1.26 could be used by local authenticated X clients to crash the X server or execute code.	7.8	More Details
CVE-2026-128321	Tight JPEG decoding in TightVNC and UltraVNC viewers contains a heap-based buffer overflow because an attacker-controlled framebuffer rectangle width is not validated against a fixed-size decoding buffer. A malicious VNC server can cause an out-of-bounds heap write when a user connects, resulting in application crash and potentially other memory-corruption impacts.	7.8	More Details
CVE-2026-124003	XWEB EVO before 5.6.2 contains a command injection vulnerability where the setuid-root Lua CGI interpreter wlua executes system("/usr/bin/lua "+argv) on unsanitized input. Attackers can craft malicious input reached through a .lua CGI endpoint to inject arbitrary commands into the concatenated argv string, achieving command execution with root privileges. This product line reached it's end of service date in March 2026.	7.8	More Details
CVE-2026-124705	In Progress® Telerik® UI for .NET MAUI prior to version 16.0.0, an untrusted URL redirection vulnerability in the RadRichTextEditor hyperlink handling and the RadPdfViewer link annotation handling allows an unauthenticated attacker to launch arbitrary operating system protocol handlers with attacker-controlled arguments via a crafted document or PDF link with a non-allowlisted URI scheme that the user opens.	7.8	More Details
CVE-2026-49747	Software installed and run as a non-privileged user may conduct GPU system calls to trigger an integer overflow and allow OOB writes to GPU buffers. The integer overflow caused when mapping a GPU buffer >4GB causes corruption of array length, and can lead to kernel panics or out of bounds access.	7.8	More Details
CVE-2026-91007	The user-mode syscall verifiers for the charger driver API in drivers/charger/charger_handlers.c did not inspect the prop argument before copying union charger_propval across the user/kernel boundary. Two members of that union are function pointers — status_notification (CHARGER_PROP_STATUS_NOTIFICATION) and online_notification (CHARGER_PROP_ONLINE_NOTIFICATION), declared in include/zephyr/drivers/charger.h — and z_vrfy_charger_set_prop() forwarded the caller-supplied union verbatim to the driver's set_property callback for any property. z_vrfy_charger_get_prop() had the mirror defect and copied the stored kernel callback address back out to user memory. With CONFIG_USERSPACE enabled, any user-mode thread that has been granted a charger device object could call charger_set_prop() with CHARGER_PROP_STATUS_NOTIFICATION or CHARGER_PROP_ONLINE_NOTIFICATION and an arbitrary pointer value. Drivers that implement these properties — drivers/charger/charger_max20335.c, drivers/charger/charger_pf1550.c and drivers/charger/charger_bq2518x.c — store the pointer in device data and later invoke it from their interrupt work handlers, which run in supervisor mode, on any charger state change such as a cable plug/unplug. The result is a control-flow hijack at kernel privilege from an unprivileged thread, defeating the isolation that CONFIG_USERSPACE is meant to provide; the read path additionally disclosed a kernel code address to user mode, and clearing a notifier installed by a supervisor thread let user mode suppress charger notifications. Supervisor-mode callers of charger_set_prop()/charger_get_prop() are unaffected. The fix makes both verifiers reject the two notifier properties outright — including when the supplied callback is NULL, since the notifiers are device state — and adds a BUILD_ASSERT on CHARGER_PROP_COMMON_COUNT so that new properties force a re-review of the union's user-mode safety.	7.8	More Details
CVE-2026-124704	In Telerik UI for WPF, versions prior to 2026.4.1110, a deserialization of untrusted data vulnerability exists that allows an attacker to perform unauthorized actions in the context of the affected application.	7.8	More Details
CVE-2026-126862	Improper input validation in Core in Google Chrome on on Android prior to 157.0.8103.78 allowed a local attacker to bypass web origin policy via a co-installed app. (Chromium security severity: High)	7.7	More Details
CVE-2026-107443	A flaw was found in Foreman. An authenticated user with view_hosts privileges can retrieve rendered provisioning template content for a host via the hosts template API endpoint, disclosing sensitive data such as the host root password. This is an incomplete fix of CVE-2026-96659, which hardened the web UI preview path but left the API host-template render path authorized for Viewer-level users.	7.7	More Details
CVE-2026-126488	OpenEMR before 8.5.0 contains an SQL injection vulnerability in the patient portal OnsiteDocument.Query endpoint, where mass-assigned _BitwiseAnd criteria parameters are placed unquoted into SQL with only quote-character escaping. Authenticated portal patients can inject SQL outside their per-patient scope to read the entire database, including other patients' demographics and users_secure password hashes.	7.7	More Details
CVE-2026-127082	Huginn before 2026.11.09 contains an information exposure vulnerability in JqAgent that allows authenticated users to read the server process environment because the jq child process inherits it. Attackers who can create, configure or dry-run a JqAgent can supply a filter using env or $ENV to disclose APP_SECRET_TOKEN, database, SMTP and OAuth secrets.	7.7	More Details
CVE-2026-128329	Dokploy 0.28.0 before 0.31.1 contains a path traversal vulnerability that allows authenticated organization members to read arbitrary files by supplying ../ sequences in the filePath of patch.readRepoFile. Attackers with service read permission can read /etc/shadow, SSH private keys, and secret environment files on the Dokploy host or managed remote servers.	7.7	More Details
	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.6, 1.5.2, and 1.6.1, the BACnet/SC message decoder walks the header-option list by following each option's MORE bit. Nothing rejects a list whose last option still has the MORE bit set, and the decode walk has no upper bound		

CVE-2026-97692	on how many options it processes. A single crafted BVLC-SC frame makes the walk advance one option past the end of the message and read message[message_len], one byte out of bounds. When the bytes after the message carry more MORE-set option markers, the walk keeps going: it runs past the fixed 4-entry option array and writes decoded option fields out of bounds. On the server that decode array is the static global bsc_dm, so the out-of-bounds write lands in adjacent BSS. Both faults are reachable before authentication, from the first frame a peer sends on a BACnet/SC connection, and the bytes that follow the message are the same peer's prior-frame data. This issue has been patched in versions 1.4.6, 1.5.2, 1.6.1, and 1.7.0.	7.7	More Details
CVE-2026-128044	OpenMage magento-lts before 20.18.2 and 21.x before 21.0.0-beta3 validates OAuth 1.0a oauth_callback URLs with a string-prefix check and falls back to accepting any well-formed URL. Attackers holding a leaked consumer key and secret can supply host-suffix, userinfo, or arbitrary callback URLs to capture an approving administrator's or customer's request token and verifier, then obtain an access token with the victim's API privileges.	7.7	More Details
CVE-2026-105153	Improper Restriction of XML External Entity Reference in Apache Roller 4.0 through 6.1.6 allows an authenticated user with no weblog permissions to read files readable by the Roller process and cause the server to issue outbound HTTP requests to attacker-chosen destinations, by submitting a crafted Atom entry to the AtomPub endpoint. The entry body is parsed with a parser configuration that permits external parameter entities and external DTD subsets, and the parse happens before any per-weblog authorization check and before any check of whether the AtomPub feature is enabled, so the endpoint is reachable by any authenticated account on a default installation. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which parses AtomPub entries with a hardened XML configuration and rejects AtomPub requests while the feature is disabled.	7.7	More Details
CVE-2026-125852	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Realtyna Realtyna Organic IDX plugin real-estate-listing-realtyna-wpl allows Path Traversal.This issue affects Realtyna Organic IDX plugin: from n/a through 5.5.0.	7.7	More Details
CVE-2026-126271	NocoDB before 2026.09.0 contains an information disclosure vulnerability that allows authenticated base Viewers to obtain TLS client private keys by reading a base's data source. The source read handler masked only the connection password, letting attackers retrieve the decrypted private key, client certificate and CA to connect directly to the external database, bypassing NocoDB permissions.	7.7	More Details
CVE-2026-126264	SiYuan before 3.8.9 contains an information disclosure vulnerability that allows authenticated Reader users to retrieve credential-named widget files by bypassing the sensitive-path guard in getFile. Attackers can request paths like /data/widgets/<package>/credentials.json for publish-referenced widgets to obtain API keys, tokens, or other stored secrets.	7.7	More Details
CVE-2024-58404	Zipline versions from 3.4.5 before 3.7.10 contain a path traversal vulnerability in the user data export endpoint via the name query parameter. Authenticated attackers can bypass the user id check and use directory traversal sequences to read arbitrary files on the server host.	7.7	More Details
CVE-2026-126385	n8n before 2.45.5, 2.46.x before 2.46.1, and 3.x before 3.0.1 contains a flaw in the OAuth2 credential callback of the dynamic-credential connect flow, which does not verify that the completing browser belongs to the user who started the flow. Members with access to a resolvable OAuth2 credential can send the provider authorization URL to a victim; if the victim consents without an active n8n session, the victim's tokens are stored under the member's identity, letting the member's workflows act as the victim.	7.7	More Details
CVE-2026-126285	NocoDB before 2026.08.0 contains an sql injection vulnerability that allows authenticated users with read access to run arbitrary read queries via the legacy where parameter on PostgreSQL. Attackers, including Viewer-role users, can inject single quotes into filter values concatenated by CustomKnex.ts to read other tables, schemas, view-filtered rows, and hidden columns.	7.7	More Details
CVE-2026-126308	The web dashboard in Coder 2.24.0 before 2.29.23, 2.30.0 before 2.34.14, 2.35.0 before 2.36.9, 2.37.0 before 2.37.6, and 2.38.0 before 2.38.2 replaces the $SESSION_TOKEN placeholder in external app URLs with a full-access API key without checking whether the app belongs to a sub-agent. Code running in a workspace can register a disguised sub-agent app with a custom protocol URL, so the owner's click sends their API key to an attacker-chosen destination.	7.7	More Details
CVE-2026-127094	Pagelayer 2.1.7 before 2.2.1 contains a missing authorization vulnerability in Abilities API abilities registered in main/abilitiesregister.php that only require the edit_posts capability. Contributor-level attackers can overwrite, publish, delete, or duplicate other users' private posts and pages to read them, and modify site-wide theme templates like headers and footers.	7.6	More Details
CVE-2026-126479	OpenEMR before 8.5.0 contains a missing authorization vulnerability in five Module Manager InstallerController actions that lack the admin/manage_modules ACL check and CSRF validation. Low-privilege users such as Front Office accounts can POST to saveConfig or SaveHooks to overwrite any module's configuration, retarget CCDA and HIE settings, and delete module hooks.	7.6	More Details
CVE-2026-126570	Padloc 4.0.0 before 4.3.1 contains a prototype pollution vulnerability that allows SCIM token holders to modify Object.prototype by sending crafted SCIM PATCH paths to ScimServer._handleScimUsersPatch(). Attackers can supply paths like __proto__.x or constructor.prototype.x passed to setPath() to pollute the shared server process, disrupting requests for all other organizations.	7.6	More Details
	AsiaInfo BSS Platform 9.2 before 9.2.38 has a stored cross-site scripting (XSS) vulnerability in the menu icon		

CVE-2026-122095	upload function. An authenticated user with ordinary application privileges can upload an SVG file containing embedded JavaScript, which is served from the application origin. Normal menu rendering uses an HTML <img> element and does not execute the SVG script; exploitation requires a victim to load the uploaded SVG as a document (by directly navigating to its URL, or via <object>/<iframe>), in which case the script executes under the application origin.	7.6	More Details
CVE-2026-126379	Vvveb 1.0.8.6 contains an incomplete server-side request forgery fix that allows authenticated admin users to bypass DNS pinning by requesting non-443 URLs. Attackers can supply a rebinding hostname to the editor oEmbedProxy url parameter to read loopback services, internal panels, and cloud metadata credentials.	7.6	More Details
CVE-2026-91877	Dell OpenManage Ansible Modules, versions 2.0.2 through 10.0.3, contains an Improper Neutralization of Special Elements in Data Query Logic vulnerability in the OData filter processing component. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized data access, authorization bypass, and denial of service.	7.6	More Details
CVE-2026-65971	Livewire PowerGrid creates data tables based on Laravel Livewire library. From version 6.0.0 to before version 6.10.4, the public Livewire property sortDirection is interpolated verbatim into a raw SQL ORDER BY clause and is not restricted to asc/desc, allowing arbitrary SQL injection through POST /livewire/update. This issue has been patched in version 6.10.4.	7.6	More Details
CVE-2026-124741	A flaw was found in BusyBox. The udhcpc6 DHCPv6 client does not properly validate the size of network options sent by a server before copying them into memory. A malicious DHCPv6 server on the local network can exploit this flaw by sending a crafted reply, triggering a stack-based buffer overflow. This vulnerability could allow an attacker to achieve arbitrary code execution with root privileges or cause a denial of service (DoS) crash.	7.6	More Details
CVE-2026-126152	A authorization bypass through user-controlled key vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an authenticated remote attacker to delete arbitrary directories as root, or to access or delete other users' calendar and mailbox data across tenant domains, via crafted HTTP requests to the webmail and administrative interfaces.	7.6	More Details
CVE-2026-126486	OpenEMR before 8.5.0 contains a missing authorization vulnerability in portal/import_template.php, where several portal document template modes lack admin/forms ACL and CSRF checks. Any authenticated staff user can send mode=save_profiles to delete all template profile assignments, use other unguarded modes to push templates to patients or change categories, and read template bodies via mode=get or getPdf.	7.6	More Details
CVE-2026-126491	OpenEMR before 8.5.0 contains a stored SQL injection vulnerability in getByPatientDemographics() where layout_options field_id values are concatenated into the patient search WHERE clause. Attackers with Layout Editor access can plant a malicious field_id, allowing any authenticated low-privilege user to exfiltrate data from patient_data and users_secure tables.	7.6	More Details
CVE-2026-91878	Dell OpenManage Ansible Modules, versions 6.0.0 through 10.0.3, contains an Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in the XML data conversion component. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to XML injection, malicious content injection, and XML parsing errors	7.6	More Details
CVE-2026-126478	OpenEMR before 8.5.0 contains an SQL injection vulnerability in the Syndromic Surveillance report because the form_icd_codes[] POST array is concatenated into an unquoted numeric IN() clause without integer validation. Authenticated users can submit quote-free payloads that bypass add_escape_custom to perform blind or UNION-based injection and exfiltrate patient health information.	7.6	More Details
CVE-2026-126915	Use of uninitialized variable in Skia in Google Chrome on on Android prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-129122	C-Kermit 6.0.192 before 11.1.515 contains a buffer overflow vulnerability in tn_snenv() in ckctel.c that allows malicious Telnet servers to corrupt client memory via crafted NEW-ENVIRON SEND subnegotiation. Malicious or machine-in-the-middle servers can send oversized variable names before authentication, overflowing a 16-byte stack buffer and a miscomputed heap buffer to corrupt stack and heap memory.	7.5	More Details
CVE-2026-129151	SurveyKing 1.13.2 contains a missing authorization vulnerability in result lookup: the anonymous survey view leaks the lookup configuration, including its password, and the lookup password check is skipped when no answer is sent. Unauthenticated attackers with a public survey link can inject a % wildcard into the MyBatis LIKE condition to match all responses, then call loadProject with an answerId to read complete responses including hidden fields.	7.5	More Details
CVE-2026-126244	A allocation of resources without limits or throttling vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to exhaust system resources, potentially resulting in a denial of service (DoS).	7.5	More Details
CVE-2026-129143	paicoding 1.0.3 contains a missing authorization vulnerability in the ArticleRestController article detail endpoint that allows unauthenticated attackers to read restricted articles. Attackers can enumerate article IDs via GET /article/api/data/detail/{articleId} to retrieve full content of paid, login-only, member-only and draft articles.	7.5	More Details
CVE-2026-	A null pointer dereference vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to perform a denial of service attack via http	7.5	More

126246	requests.		Details
CVE-2026-126248	A insufficiently protected credentials vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to obtain sensitive information via HTTPS requests.	7.5	More Details
CVE-2026-126258	A stack-based buffer overflow vulnerability in Fortinet FortiOS 8.0.0, FortiOS 7.6.7 may allow an unauthenticated attacker with wad port access to crash proxy or ZTNA sessions via crafted HTTP or HTTPS requests.	7.5	More Details
CVE-2026-18633	An access of uninitialized pointer vulnerability in the nfsd in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers to conduct denial-of-service attacks.	7.5	More Details
CVE-2026-123097	The WP Remote Users Sync WordPress plugin before 2.2.1 does not restrict which account fields a synchronised site may set when it creates or updates users, allowing a site holding the shared synchronisation keys to assign the administrator role, modify any existing account and write arbitrary user metadata, bypassing the receiving site's role and metadata restrictions.	7.5	More Details
CVE-2026-128120	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From version 2.42.0 until 3.1.1, applications using the experimental remote functions flag and a remote form function could perform quadratic synchronous work while parsing a specially crafted request with many form entries. The parsing work could block the event loop for an extended period and deny service. This issue is fixed in 3.1.1.	7.5	More Details
CVE-2026-128118	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From version 3.0.0 until 3.1.1, the build-time server-only module guard did not treat src/params.js as a client entry point even though parameter matchers can run in the browser. Server-only modules imported through src/params.js could consequently enter the client bundle, where statically replaced private environment values or other server secrets could be exposed. This issue is fixed in 3.1.1.	7.5	More Details
CVE-2026-124739	A flaw was found in BusyBox. When the httpd web server processes subdirectory configuration files, an overly long index page name can trigger a stack-based buffer overflow. An attacker with permissions to write to a subdirectory configuration file could exploit this vulnerability to execute arbitrary code with elevated privileges or cause a denial of service (DoS) by crashing the server process.	7.5	More Details
CVE-2026-49341	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to version 1.5.1, there is a remotely reachable denial-of-service vulnerability in bacnet-stack affecting the default demo server built from the unmodified apps/server/main.c. This issue has been patched in version 1.5.1.	7.5	More Details
CVE-2026-90993	XXE vulnerability in Apache XML Graphics Batik. This issue affects Apache XML Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.	7.5	More Details
CVE-2026-47217	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4 and 1.5.1, a remote attacker can trigger an uncontrolled recursion and stack overflow in the default server application of bacnet-stack by abusing the Channel object. This issue has been patched in versions 1.4.4 and 1.5.1.	7.5	More Details
CVE-2026-126401	Fleet before 4.86.2 contains a denial of service vulnerability that allows unauthenticated attackers to exhaust server memory through quadratic XML canonicalization of unsigned SAML responses. Attackers can send a single crafted SAML response with deeply nested elements declaring new namespace prefixes to POST /api/v1/fleet/sso/callback, crashing the Fleet server.	7.5	More Details
CVE-2026-118065	The Advance Guest Post WordPress plugin through 1.9 does not perform any authorization or ownership check when deleting media attachments, relying only on a nonce exposed to every site visitor, allowing unauthenticated users to permanently delete arbitrary Media Library attachments and their files.	7.5	More Details
CVE-2026-116418	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains an Incorrect Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.5	More Details
CVE-2026-124737	A flaw was found in BusyBox. When the TFTP (Trivial File Transfer Protocol) client requests a custom small block size and receives a standard response, it falls back to the default block size without resizing the allocated memory buffer. A malicious TFTP server can exploit this issue by sending standard-sized network packets during a transfer, causing a heap buffer overflow. This flaw allows an attacker to achieve arbitrary code execution or cause a Denial of Service (DoS) by crashing the application.	7.5	More Details
CVE-2026-126239	A stack-based buffer overflow vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to crash the FSSO subsystem via crafted http requests	7.5	More Details
CVE-2026-125799	Insertion of Sensitive Information into Externally-Accessible File or Directory vulnerability in Looks Awesome Flow-Flow Social Stream flow-flow-social-streams allows Retrieve Embedded Sensitive Data.This issue affects Flow-Flow Social Stream: from n/a through 5.0.5.	7.5	More Details

CVE-2026-126902	Incorrect reference resolution in Browser in Google Chrome on on Mac prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-126397	vLLM from 0.10.1 before 0.31.0 forwards a request-controlled mm_processor_kwargs.max_patches value to the Hugging Face processor for Cohere2 Vision models without a server-side upper bound, causing quadratic CPU work during multimodal preprocessing. Remote clients can send small image chat-completion requests with large, varying max_patches values to bypass the LRU cache, exhaust preprocessing workers, and deny service to other clients.	7.5	More Details
CVE-2026-126266	SiYuan from 3.6.0 before 3.8.9 contains an information disclosure vulnerability that allows unauthenticated publish visitors to bypass per-document passwords via regex search in getDoc. Attackers can send POST requests to /api/filetree/getDoc with queryMethod 3 and a broad regex to read protected body text returned in the unfiltered keywords field.	7.5	More Details
CVE-2026-126191	Soup Sieve is a CSS selector library designed to be used with Beautiful Soup 4. Prior to 3.0, the CSS_ESCAPES and IDENTIFIER regular-expression subpatterns can backtrack exponentially on runs of ambiguous digit escapes in an attribute-name or tag position of an otherwise valid selector. The failure occurs during selector compilation through soupsieve.compile() or Beautiful Soup select() before SELECTOR_LIMIT is applied, so an application that accepts untrusted selector strings can have a worker stalled by a short input. This issue is fixed in version 3.0.	7.5	More Details
CVE-2026-126621	Progressive Robot hMailServer 6.0.0-B1 through 6.3.7 on Windows hands OpenSSL the names of its own TLS files - the listeners' certificates, chains, private keys and Diffie-Hellman parameters, a port's client-certificate CA file (from 6.2.19), the object store's CA file (from 6.3.4) and the ACME client's keys and certificates - as Latin-1 bytes, which on code page 1252 are the code page's own for U+00A0 to U+00FF, and OpenSSL's file opening on Windows reads a name as UTF-8 first and opens the file at that reading when it is there, or creates it there when its folder is. When every byte of a configured name outside ASCII also reads as UTF-8 - for example U+00C3 U+00A9, the bytes C3 A9, which are U+00E9 in UTF-8 - the server used the file at that other name whenever one was there, which allows a local attacker who can create that file or its folder but cannot change the configured one, as any user can by default beside a file an administrator keeps under ProgramData, to have a port that logs on by client certificate (from 6.2.25) accept certificates from a certificate authority of the attacker's own and so sign in over the network as any mailbox without its password; to have the server trust such an authority for its object store and, intercepting that connection, read and modify the messages it stores; to receive the private keys the ACME client writes, the key of a certificate issued for the server's names among them; or to keep TLS ports from starting. The configuration is not the default: by default these files have names in ASCII, client certificates are off on every port, and the object store and ACME are off. The Linux builds are not affected.	7.5	More Details
CVE-2026-123092	The WP Remote Users Sync WordPress plugin before 2.3.0 does not restrict which user metadata keys may be written through its incoming user synchronisation requests, allowing a site that holds the shared synchronisation keys to set the capabilities of any existing account and escalate it to administrator.	7.5	More Details
CVE-2026-126779	Spatie Browsershot 2.2.0 before 5.5.0 contains a local file read vulnerability that allows attackers to read server files by supplying root-relative references in HTML passed to setHtml(). Attackers can embed iframe, img, link or script elements referencing paths like /etc/passwd, which resolve to file:// URLs and render file contents into the returned PDF or screenshot.	7.5	More Details
CVE-2026-126623	Inefficient algorithmic complexity in the JSON reader of Progressive Robot hMailServer 6.3.6 and 6.3.7 allows a remote attacker to hold the server's mail delivery threads or its REST API's worker threads, making mail delivery, the REST API and the webmail unavailable. 6.3.6 fixed CVE-2026-107574, in which reading a JSON object searched the member names already read for each new name, by keeping the names in a hash set; the set uses the standard library's hash, which takes no secret, so member names chosen to fall in one bucket of it still cost time growing with the square of their number. Against the released reader, one such object of 16 MB took about 5 seconds to read in the Linux build, and one of under 6 MB about 23 seconds in the Windows build, where objects of the same sizes with other names took under a tenth of a second. A remote unauthenticated attacker reaches the reader by mailing such an object as a TLS-RPT report, up to 16 MB once decompressed, to a hosted domain's report mailbox, where an administrator has set one; it is read on a mail delivery thread (ten by default), and those threads deliver all mail, local and outbound, so a stream of such reports stops all delivery for as long as it continues. It is also reached without an account through the reply to a password-protected message, with the message's link alone, where the REST API is on (it is off by default) and a public base URL for such links is set; and by any account through the webmail's routes granted 16 MB, and by an application's API key through the send API. Each such request holds one of the REST API's four worker threads, in the process that also serves SMTP, IMAP and POP3.	7.5	More Details
CVE-2026-63151	Omnispace Agora Project through 26.10.0 contains a predictable token generation vulnerability that allows unauthenticated attackers to access private calendar data by exploiting a missing dateCrea value that causes the md5Id token to collapse to md5(calendarId.userId), both small enumerable integers. Attackers can compute valid tokens and request the misc&action=DisplayIcal endpoint with a forged md5Id to read any user's private calendar events without authentication.	7.5	More Details
CVE-2026-	The WooCommerce Vindi Pagamento WordPress plugin through 0.8.3 does not perform any authorisation check when updating an order's shipment tracking code, and does not escape that code when displaying it on the order edit page, allowing unauthenticated attackers to perform Stored Cross-Site Scripting attacks against	7.5	More

123124	administrators and shop managers who view an order paid through the gateway. The stored payload is only rendered on sites using WooCommerce's legacy (WordPress posts) order storage.		Details
CVE-2026-119040	The Defender Security WordPress plugin before 6.4.1 does not limit the number of failed two-factor authentication attempts in its default configuration, allowing an attacker who already knows a victim's password to brute-force the one-time code and defeat the second authentication factor.	7.5	More Details
CVE-2026-127029	A flaw was found in freeradius's Extensible Authentication Protocol Method for Subscriber Identity Module (EAP-SIM) module. When handling authentication requests, the server copies a client-supplied identity into an internal structure without properly checking its length against a fixed-size buffer. An unauthenticated remote attacker can exploit this issue by sending specially crafted EAP-SIM messages, triggering a stack buffer overflow that crashes the service and results in a Denial of Service (DoS).	7.5	More Details
CVE-2026-126232	A improper certificate validation vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow a MITM attacker to impersonate the radius server via a rogue RADIUS server.	7.5	More Details
CVE-2026-127030	A flaw was found in freeradius. An improper length validation in the EAP-FAST module allows a stack-based buffer overflow during session ticket processing. A remote, unauthenticated attacker can exploit this flaw by sending a specially crafted handshake request, causing the server process to crash and resulting in a Denial of Service (DoS).	7.5	More Details
CVE-2026-126904	Use after free in Compositing in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-128128	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, the C WebSocket reader adds a declared frame length to the size of an already buffered partial message using signed 64-bit arithmetic. A length near two to the power of 63 can overflow, allowing the max_msg_size check to pass. A remote peer can send a small non-final fragment followed by an oversized message and cause unbounded memory consumption. The Python WebSocket reader is unaffected. This issue is fixed in version 3.14.4.	7.5	More Details
CVE-2026-126237	A loop with unreachable exit condition ('infinite loop') vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an attacker to cause a denial of service via crafted TCP requests.	7.5	More Details
CVE-2026-121737	When a remote, unauthenticated HTTP/1.1 client pipelined the start of a second request and then stopped reading, proxygen's coroutine-based HTTP session could free that pipelined stream while resetting the connection's streams on the resulting write timeout, then go on to use it. This can crash the server, leading to denial of service, and may allow memory corruption with further impact. This issue affects proxygen versions prior to v2026.11.09.00.	7.5	More Details
CVE-2026-119723	When parsing request variables such as query-string and form parameters, HHVM did not check that appending a nested array succeeded before descending into it. A remote, unauthenticated attacker could send a GET or POST request which would crash the HHVM server process before any application code runs, leading to denial of service. This issue affected HHVM prior to 23c061f4e804a51badd5f85227e65185651253b5.	7.5	More Details
CVE-2026-119237	In proxygen's HTTP/3 session, when a HEADERS block referenced QPACK dynamic table entries that had not yet been received, header decoding for that stream was paused, but the session continued to read the stream from the QUIC transport. The unread data bypassed the session's ingress buffer limit, returned flow-control credit to the peer, and was re-scanned in full on every read. With QPACK blocked streams enabled (the default), a remote, unauthenticated HTTP/3 peer could send a HEADERS block that references a dynamic table insert it never sends, followed by a continuous stream of data, causing memory growth until the request timed out and CPU usage that grows quadratically, leading to denial of service. This issue affects proxygen versions prior to v2026.11.09.00.	7.5	More Details
CVE-2026-106023	NULL pointer dereference vulnerability in Apache HTTP Server's mod_md during HTTP request processing. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.69.	7.5	More Details
CVE-2026-124541	JSON::XS versions before 4.05 for Perl leak the decoded part of a rejected long string in decode_str. A string is decoded through a fixed-size buffer (16 KiB in 4.04), and each time the buffer fills its contents move into a new scalar. Nothing frees that scalar when the string is then rejected for a control character, an invalid escape, malformed UTF-8 or the end of the input. A process that keeps running after a failed decode retains the decoded part of each rejected string, with its size chosen by the sender. Repeated requests exhaust process memory.	7.5	More Details
CVE-2026-129116	C-Kermit from 7.0.197 before 11.1.515 contains an authentication bypass vulnerability in the IKSD SSL build that leaves Telnet authentication state at AUTH_VALID after a refused certificate login. Attackers holding a trusted certificate mapped to a refused account can log in as any other account with any password, gaining that account's shell access.	7.5	More Details

CVE-2026-126384	n8n before 1.123.89, 2.x before 2.45.5, 2.46.x before 2.46.1, and 3.x before 3.0.1 bundles a GraphicsMagick version with known vulnerabilities in its official Docker image, which the Edit Image node uses to process images. Attackers who can supply crafted untrusted images to an Edit Image workflow, such as one fed by a Webhook node, can execute code on the n8n instance.	7.5	More Details
CVE-2026-75492	Cudy TR3000 before 2.5.42 contains an unauthenticated stack buffer overflow vulnerability in the stun_client TR-111 UDP Connection Request parser that parses requests before verifying username or HMAC. Remote attackers can send a single crafted UDP datagram lacking a space in the request line, causing strncpy() to overflow a 10-byte stack buffer and crash stun_client for denial of service.	7.5	More Details
CVE-2026-75490	Cudy TR3000 before 2.5.42 contains a remote code execution vulnerability that allows unauthenticated adjacent attackers to run root commands by advertising a rogue automesh controller over mDNS. Attackers on the upstream Ethernet segment can advertise _cudycmagent._tcp records pointing to a malicious MQTT broker, then send commands encrypted with a fixed AES key that router/batchcmd.lua executes as root.	7.5	More Details
CVE-2026-122096	Uncontrolled Resource Consumption vulnerability in the sketch deserialization of Apache DataSketches Java. Several deserializers trusted sizes and counts declared in the serialized input. A small crafted input could make an application allocate an excessive amount of memory, leading to an OutOfMemoryError. A crafted string passed to FrequentLongsSketch.getInstance(String) could also make deserialization, or a later update, loop indefinitely. Only applications that deserialize sketches from untrusted sources are affected. This issue affects Apache DataSketches Java: through 9.0.0. Users are recommended to upgrade to version 9.1.0, which fixes the issue.	7.5	More Details
CVE-2023-54423	OpenMage magento-lts before 20.2.0 contains a stored cross-site scripting vulnerability because the TinyMCE WYSIWYG editor fails to filter scripts in specially crafted HTML tags. Attackers can inject an img element with a malicious onmouseover attribute to execute scripts in the browsers of users viewing the rendered content.	7.5	More Details
CVE-2026-52789	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, a Denial of Service (DoS) vulnerability exists in the BACnet stack's ReadPropertyMultiple (RPM) handler. When processing a malformed RPM request packet that lacks the expected closing tags, the function handler_read_property_multiple enters an infinite loop. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	7.5	More Details
CVE-2026-124536	JSON::XS versions before 4.05 for Perl allow memory exhaustion by buffering incremental input past max_size after a NUL byte in incr_parse. The parser appends each chunk to its buffer and compares max_size with how far it has progressed, not with the buffer length. It treats a NUL byte as the end of the input, so a NUL within the first max_size bytes keeps it short of the limit. The buffer keeps growing, and incr_skip cannot remove the NUL. A peer streaming data to an incr_parse consumer can exhaust process memory regardless of max_size.	7.5	More Details
CVE-2026-126091	Dental practice sites hosted with iDentalSoft send a JSON response to any user who loads certain pages containing sensitive information, including OAuth credentials, password hashes, and PII. Fixed in iDentalSoft 14.0.3.	7.5	More Details
CVE-2026-52787	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0-rc2, a reachable out-of-bounds write exists when encoding the device.address-binding property. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0-rc2.	7.5	More Details
CVE-2026-126391	n8n before 1.123.89 contains an insufficient isolation vulnerability in workflow expression evaluation that allows authenticated users to escape the sandbox. Attackers with permission to create or modify workflows can craft expressions referencing unexpected JavaScript properties to execute arbitrary code on the n8n host.	7.5	More Details
CVE-2026-61418	Dell SmartFabric OS10 Software, versions prior to 10.6.0.10, contains an Incorrect Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.5	More Details
CVE-2026-128082	AutoMapper is a convention-based object-object mapper in .NET. Prior to 15.1.4 and from 16.0.0 until 16.3.0, AutoMapper increments type depth only after creating the destination, so recursive mapping performed through constructor parameters occurs before MaxDepth is counted. Destinations built through positional records or other constructors, and recursive ConstructUsing mappings that call context.Mapper, can therefore bypass explicit MaxDepth values and the default limit of 64. Deep attacker-influenced input can throw an uncatchable StackOverflowException and terminate the process. This issue is fixed in versions 15.1.4 and 16.3.0.	7.5	More Details
CVE-2026-126877	Use after free in Dawn in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-126659	BlueprintUE Self-Hosted Edition 1.0.0 before 4.3.5 contains a resource exhaustion vulnerability that allows unauthenticated attackers to fill server storage by repeatedly creating anonymous blueprints. Attackers can send large requests to HomeController::doProcessCreateBlueprint() with a 'never' expiration, bypassing purges to fill the disk and deny service.	7.5	More Details
CVE-2026-	JSON::XS versions before 4.05 for Perl allow stack exhaustion via nested tagged values under allow_tags in decode_tag. With allow_tags, "(" starts a tagged value. Its tag and value are decoded recursively, and each can start another tagged value. Unlike arrays and objects, this nesting is not counted against max_depth. A run of "("	7.5	More Details

124540	bytes exhausts the C stack and triggers an uncatchable segmentation fault regardless of max_depth.		
CVE-2026-127204	WooCommerce PayPal Pro Payment Gateway plugin before 4.1.1 contains an unauthenticated payment bypass vulnerability that allows remote attackers to mark unpaid orders as paid by exploiting the pp_capture_order AJAX handler, which is gated only by a public checkout nonce and fails to properly validate the PayPal capture response status. Attackers can supply a valid _paypal_order_id to trigger payment_complete() without verifying the capture status or amount, causing the store to fulfill goods or services that were never paid for and resulting in direct financial loss to the merchant.	7.5	More Details
CVE-2026-46674	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4 and 1.5.1, an out-of-bounds read vulnerability exists in bacnet-stack's AtomicWriteFile record-access path. The bug is caused by a mismatch between an externally controlled returnedRecordCount field and the fixed-size internal fileData[] array used by BACNET_ATOMIC_WRITE_FILE_DATA. This issue has been patched in versions 1.4.4 and 1.5.1.	7.5	More Details
CVE-2026-119236	An mvfst QUIC server retained CRYPTO frame data received at an encryption level (Initial or Handshake) that the TLS handshake had already moved past. Because the transport treated this data as delivered, it did not count against the CRYPTO stream buffer limit. A remote, unauthenticated client could complete a handshake, withhold its acknowledgment of the server's HANDSHAKE_DONE frame so that Handshake keys stay in use, and keep sending Handshake-level CRYPTO data at increasing offsets, causing unbounded memory growth on the server and leading to denial of service. This issue affects mvfst versions prior to v2026.11.09.00.	7.5	More Details
CVE-2026-45341	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. From versions 1.4.0 to before 1.4.4, and 1.5.0 to before 1.5.1, a NULL pointer dereference can be triggered in bacnet_device_object_reference_decode() when a WriteProperty request updates OBJECT_STRUCTURED_VIEW / PROP_SUBORDINATE_LIST. This issue has been patched in versions 1.4.4 and 1.5.1.	7.5	More Details
CVE-2026-68538	fulgur converts untrusted HTML/CSS into PDF, commonly on a server that processes input supplied by many tenants. From version 0.15.0 to before version 0.27.0, resolving the CSS counters(name, sep) function in generated content was bounded neither in the size of a single expansion nor in the aggregate work across an element tree. An attacker able to submit HTML/CSS to a fulgur-based conversion service can trigger CPU and memory exhaustion with a trivially small payload, denying service to the host and any co-tenants. This issue has been patched in version 0.27.0.	7.5	More Details
CVE-2026-68539	fulgur converts untrusted HTML/CSS into PDF, commonly on a server that processes input supplied by many tenants. From version 0.4.4 to before version 0.29.0, the CSS string-set named-string values resolved from a document were accumulated per element with no memory budget, letting a small crafted document amplify into large retained memory (and the CPU to copy it) — results in a denial of service. This issue has been patched in version 0.29.0.	7.5	More Details
CVE-2026-68540	fulgur converts untrusted HTML/CSS into PDF, commonly on a server that processes input supplied by many tenants. From version 0.6.0 to before version 0.33.0, quadratic style-list reprocessing during containing-block resolution for absolutely-positioned pseudo-elements cause denial of service. This issue has been patched in version 0.33.0.	7.5	More Details
CVE-2026-124649	The Lightbox with PhotoSwipe WordPress plugin before 5.19.0 does not properly sanitise link titles and other caption sources before inserting them as HTML into the image lightbox caption, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks via comments.	7.5	More Details
CVE-2026-126883	Use after free in Core in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-100403	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.6, 1.5.2, and 1.6.1, the BACnet/SC hub's Linux WebSocket server reassembles fragmented WebSocket messages into a per-connection fragment_buffer. It grows that buffer with realloc() on every non-final frame, with no upper bound. A peer that streams binary continuation fragments and never sets FIN keeps the hub reallocating until the box runs out of memory or the process is OOM-killed. The buffer starts at the maximum legal BVLC-SC NPDU size, but nothing after that ties its growth back to that limit. This issue has been patched in versions 1.4.6, 1.5.2, 1.6.1, and 1.7.0.	7.5	More Details
CVE-2026-126190	Soup Sieve is a CSS selector library designed to be used with Beautiful Soup 4. Prior to 4.0, Soup Sieve repeatedly walks the same ancestors while matching descendant combinators, and each additional descendant combinator raises the polynomial degree of the work on deeply nested attacker-influenced HTML or XML. Applications using selectors such as section div div through select(), select_one(), or Beautiful Soup CSS APIs against untrusted documents can have a worker occupied for seconds or minutes, while trusted-only document processing is not affected. Selectors compiled with NOCACHE continue to use the old uncached behavior. This issue is fixed in version 4.0.	7.5	More Details
CVE-2026-44929	Server-Side Request Forgery (SSRF) vulnerability in Apache XML Graphics Batik. This issue affects Apache XML Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.	7.5	More Details

CVE-2026-119235	proxygen's QPACK decoder enforced its size limit on a string literal in an encoder-stream instruction only after the entire literal had been received. A remote, unauthenticated HTTP/3 peer could send an insert instruction on the QPACK encoder stream that declares an arbitrarily large literal and then keep sending data, causing the decoder to buffer it without bound for the lifetime of the connection and exhaust memory, leading to denial of service. The issue occurs regardless of the advertised QPACK dynamic table capacity, including when the dynamic table is disabled. This issue affects proxygen versions prior to v2026.11.09.00.	7.5	More Details
CVE-2026-119234	mvfst did not adequately merge or compact out-of-order STREAM frame data, and a small received fragment could keep a much larger receive buffer alive. QUIC flow control limits the number of buffered stream bytes, but not this per-fragment memory and bookkeeping. A remote, unauthenticated QUIC peer could send many small, non-contiguous stream fragments to make an endpoint consume memory far in excess of its advertised receive window and spend increasing CPU time reassembling stream data, leading to denial of service. This issue affects mvfst versions prior to v2026.11.09.0.	7.5	More Details
CVE-2026-119233	proxygen's HTTP/3 codec buffered an incomplete non-DATA frame, such as a control-stream frame, a frame of an unknown or reserved type, or a HEADERS frame, until its entire declared length had arrived, without limiting that length, and re-scanned all buffered data each time more bytes arrived. A remote, unauthenticated HTTP/3 peer could declare a very large frame and deliver it slowly, causing unbounded memory growth and CPU usage that grows quadratically with the number of fragments, leading to denial of service. This issue affects proxygen versions prior to v2026.11.09.00.	7.5	More Details
CVE-2026-128089	dnspython is a DNS toolkit for Python. Prior to version 2.9.2, the from_text() parser for WKS records does not require the service number to be between 0 and 65535 before using it as a bitmap offset. An attacker-controlled zone file can supply a larger number, causing the service bitmap to grow to an extremely large size through inefficient repeated extension, consuming excessive memory and CPU and potentially terminating the process. Applications are affected only when they parse zone-file text whose record type and rdata are attacker controlled. This issue is fixed in version 2.9.2.	7.5	More Details
CVE-2026-62973	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, a remote out-of-bounds read exists in the official BACnet client application apps/readpropm in bacnet-stack commit e2bdbf6. When readpropm sends a legitimate ReadPropertyMultiple request to a malicious BACnet/IP peer, the peer can reply with a malformed but structurally valid ReadPropertyMultiple-ACK that drives the client into a global-buffer-overflow read on the global receive buffer Rx_Buf. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	7.5	More Details
CVE-2026-128346	ExcelJS through 4.4.0 contains a resource leak vulnerability in the streaming WorkbookReader.parse that leaves temporary files and open descriptors when sheet parsing fails or iteration stops early. Attackers can repeatedly upload malformed multi-sheet workbooks with worksheets placed before xl/sharedStrings.xml to fill the temporary directory and exhaust file descriptors.	7.5	More Details
CVE-2026-128347	ExcelJS through 4.4.0 contains an arbitrary file read vulnerability in the streaming WorkbookWriter that allows attackers to read local files by supplying crafted image filenames to addImage. Attackers can inject ../ path segments into user-controlled image paths, causing addMedia to embed any file readable by the Node.js process under xl/media in the generated workbook.	7.5	More Details
CVE-2026-126613	Allocation of resources without limits in the JSON reader of Progressive Robot hMailServer 6.3.2 through 6.3.7 allows a remote attacker to exhaust the server's memory and hold its threads, making mail delivery, the REST API and the webmail unavailable. The reader built a tree of values far larger than the text it read, copying each value into every level above it, and set no bound on the number of values, so a single JSON document of many small values, within the 16 MB the server reads, raised the service's memory by about 2 GB and held one thread for seconds to minutes. From 6.3.4 a remote unauthenticated attacker reaches the reader by mailing such a document as a TLS-RPT report, up to 16 MB once decompressed, to a hosted domain's report mailbox, where an administrator has set one; it is read on a mail delivery thread (ten by default), and those threads deliver all mail, local and outbound. From 6.3.4 it is also reached without an account through the reply to a password-protected message, with the message's link alone, where the REST API is on (it is off by default) and a public base URL for such links is set; and by any account, from 6.3.2 through the webmail's send and draft routes and from 6.3.4 through its other routes granted 16 MB and the send API; the webmail's send, draft and settings routes parsed the body again for each member read. The REST API serves every request on four worker threads, in the process that also serves SMTP, IMAP and POP3, so a few such documents at once make it unavailable and can exhaust the machine's memory and end the whole service. This is a separate defect from CVE-2026-107574, the reader's handling of duplicate member names, fixed in 6.3.6.	7.5	More Details
CVE-2026-123044	The ContentPen WordPress plugin before 1.1.1 discloses its REST API key to unauthenticated users, who can then use it to create posts containing unfiltered JavaScript, leading to Stored XSS that executes in the browser of any visitor, including administrators.	7.5	More Details
CVE-2026-121870	The Simpler Checkout WordPress plugin before 1.5.4 does not properly restrict who can create orders and checks its automatic login link with a key that stays empty until the store owner configures the Simpler Checkout WordPress plugin before 1.5.4, allowing subscribers on stores that have not completed setup to log in as an administrator.	7.5	More Details
CVE-2026-124267	Missing Authorization vulnerability in Noor Alam Gmail SMTP gmail-smtp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gmail SMTP: from n/a through 1.2.3.23.	7.5	More Details

CVE-2026-126298	NLTK before 3.10.4 contains a denial of service vulnerability in Tree.chomsky_normal_form that allows remote attackers to exhaust CPU through quadratic-time right-factor binarization using list.pop(0). Attackers can supply a wide flat treebank tree parsed by Tree.fromstring to force tens of seconds of single-threaded CPU consumption, blocking the processing thread.	7.5	More Details
CVE-2026-126297	NLTK before 3.10.4 contains a quadratic-time denial of service vulnerability in ConllCorpusReader._get_srl_instances that allows remote attackers to exhaust CPU through nested span rescans. Attackers can supply a crafted CoNLL SRL corpus with many predicates and span columns, placing the head span last, to pin a core for minutes.	7.5	More Details
CVE-2026-126294	Grav Login plugin before 3.11.0 contains an authentication bypass vulnerability that allows attackers with an account password to skip two-factor verification when the global twofa_enabled setting is off. Attackers can sign in through the /login form, remember-me cookie, or magic link to obtain a session the API plugin accepts, gaining full account permissions including super-admin control.	7.5	More Details
CVE-2026-126799	Gotenberg 8.31.0 before 8.38.0 contains a server-side request forgery vulnerability in IsPublicIP() that allows unauthenticated attackers to bypass private-IP deny-list protections using IPv6 zone identifiers. Attackers can append a zone such as %25eth0 to the unspecified address or blocked IPv6 prefixes in downloadFrom, webhook, or Chromium/LibreOffice URLs to reach internal services and read responses in the returned PDF.	7.5	More Details
CVE-2026-128340	ExcelJS through 4.4.0 contains a memory exhaustion vulnerability that allows attackers to crash applications by supplying a workbook with an oversized defined-name range. DefinedNames.addEx expands ranges such as S!$A$1:$XFD$1048576 from xl/workbook.xml cell by cell, causing an uncatchable fatal heap out-of-memory error during xlsx.load().	7.5	More Details
CVE-2026-123002	Gitea accepted an unlimited number of wrong TOTP passcodes during sign-in, in the password reset flow and for Basic authentication with the `X-Gitea-OTP` header. An attacker who already knows an account's password could guess the six-digit passcode by trying codes at a high rate and sign in despite two-factor authentication. After five failed passcodes, further attempts for the account are now refused for 15 minutes.	7.5	More Details
CVE-2026-125780	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Acowebs Woocommerce Custom Product Addons Pro woo-custom-product-addons-pro allows Path Traversal.This issue affects Woocommerce Custom Product Addons Pro: from n/a through 5.9.0.	7.5	More Details
CVE-2026-123975	Grid Community Toolkit before 6.2.20261111 (globus-gss-assist before 12.9) contains a heap out-of-bounds write in globus_gss_assist_token_get_fd() triggered by SSLv2 record lengths below 3. Remote unauthenticated clients can send a crafted GSI handshake record to services like globus-gatekeeper and myproxy to corrupt heap memory and crash the service.	7.5	More Details
CVE-2026-126153	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to execute unauthorized commands via crafted requests.	7.5	More Details
CVE-2026-126436	OpenEMR before 8.5.0 contains an authorization bypass vulnerability that allows OAuth2 clients to use unregistered grant types because oauth_clients.grant_types is never enforced. Attackers can request tokens with grant_type=password to bypass the user consent screen, and disabled clients can redeem authorization codes using JWT client assertions.	7.5	More Details
CVE-2026-126366	MessagePack for Ruby is an implementation of the MessagePack binary serialization format. Prior to 1.8.7, the Java-platform msgpack gem for JRuby allocated arrays and byte buffers directly from attacker-controlled array32, str32, and bin32 declared sizes before confirming that corresponding elements or bytes were available. A short MessagePack header could therefore trigger a very large allocation or sustained heap growth when an application decoded untrusted input through MessagePack.unpack or MessagePack::Unpacker, potentially exhausting the shared JVM heap. map32 and declared counts at or above 2^31 did not use the affected allocation behavior. This issue is fixed in version 1.8.7.	7.5	More Details
CVE-2026-126982	A type allow-list bypass in the BSON serialization library of the MongoDB C# Driver allows a type-restriction check to be circumvented when polymorphic data is deserialized into loosely typed members. An unauthorized party who can supply or plant BSON/JSON data that the application later deserializes can cause the application process to instantiate .NET types outside the intended allow-list and populate them with unauthorized party-controlled values. In applications that contain a suitable gadget type, this can lead to arbitrary code execution in the context of the application, with corresponding loss of confidentiality, integrity, and availability. No special privileges beyond the ability to introduce data the application reads are required.	7.5	More Details
CVE-2026-118976	In Progress® Telerik® UI for Blazor versions v11.1.0 through v14.0.0, the demo application's Chat AI Integration example contains a relative path traversal vulnerability that could allow an attacker to read files outside of the chat attachments folder that are within the server's filesystem scope.	7.5	More Details
CVE-2026-128341	ExcelJS through 4.4.0 contains a resource exhaustion vulnerability in data-validations-xform.js that allows attackers to exhaust CPU and memory by supplying unbounded sqref ranges. Attackers can provide a small crafted workbook with a sqref of A1:XFD1048576 to make xlsx.load() iterate billions of addresses, blocking the event loop and crashing the process with an uncatchable out-of-memory error.	7.5	More Details
	NocoDB before 2026.08.1 contains a race condition vulnerability in users.service.ts that allows holders of a valid		

CVE-2026-126278	reset token to perform multiple password changes by sending concurrent reset requests. Attackers can exploit the window created by slow bcrypt hashing before the token is cleared to overwrite the owner's new password and lock them out.	7.5	More Details
CVE-2026-126149	A integer overflow or wraparound vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow a remote unauthenticated attacker to crash the daemon.	7.5	More Details
CVE-2026-126299	NLTK before 3.10.4 contains a denial of service vulnerability in the CCG lexicon parser fromstring that allows remote attackers to exhaust CPU by supplying wide inputs. Attackers can submit lexicon text with long flat bracket bodies or operator chains, triggering quadratic string re-slicing in matchBrackets and augParseCategory that blocks worker threads.	7.5	More Details
CVE-2026-128339	ExcelJS through 4.4.0 contains a memory exhaustion vulnerability in Worksheet._parseMergeCells that allows attackers to crash applications by supplying unbounded mergeCell ranges. Attackers can craft a small workbook with a mergeCell ref like A1:XFD1048576, causing xlsx.load() to create billions of Row and Cell objects and abort the process.	7.5	More Details
CVE-2026-128338	exceljs through 4.4.0 contains a memory exhaustion vulnerability that allows attackers to crash applications by supplying a worksheet col element with an unbounded max attribute. Attackers can craft a small workbook with a huge max value, causing xlsx.load() to allocate hundreds of millions of Column objects and abort the process with an uncatchable heap out-of-memory error.	7.5	More Details
CVE-2024-58406	Huatian Dynamic OA8000 collaborative office system contains an unauthenticated path traversal vulnerability in /OAapp/jsp/trace/ntkodownload.jsp, where the filename request parameter is used to locate a file without restricting access to an intended directory or rejecting traversal sequences. Attackers can supply ../ sequences to read arbitrary files from the server, such as the Tomcat configuration at ROOT/WEB-INF/web.xml, exposing sensitive configuration, source, and credential material that can enable further compromise. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-11-20.	7.5	More Details
CVE-2026-126781	Webmin through 2.670 contains a users file injection vulnerability in acl/cert_issue.cgi that allows authenticated Webmin users to inject lines by supplying unvalidated certificate DN fields containing newlines. Attackers can end a DN field with a backslash and newline to add a second root entry with a known password hash, gaining Webmin root access after miniserv restarts.	7.5	More Details
CVE-2026-126428	OpenEMR before 8.5.0 contains a remote code execution vulnerability that allows authenticated billing users to store attacker-controlled PHP by uploading a malformed ERA file to era_payments.php. Attackers with a database-write primitive such as SQL injection can register a background_services row whose require_once loads the stored .edi file, executing PHP as the web-server user.	7.5	More Details
CVE-2026-58505	geojson-vt is a JavaScript library for slicing GeoJSON data into vector tiles on the fly, primarily designed to enable rendering and interacting with large geospatial datasets on the browser side (without a server). Prior to version 6.1.1, @maplibre/geojson-vt contains an uncontrolled recursion vulnerability in its GeoJSON conversion logic. When a GeoJSONVT instance is constructed with a deeply nested GeometryCollection object, the mutually recursive functions featureToInternal and convertGeometryCollection in src/convert.ts exhaust the Node.js call stack, causing an unhandled RangeError: Maximum call stack size exceeded that terminates the process. Because the library is widely used in server-side tile services that accept GeoJSON over the network, a remote unauthenticated attacker can trigger a denial-of-service by sending a single crafted payload. No authentication is required, and no non-default library options are needed. This issue has been patched in version 6.1.1.	7.5	More Details
CVE-2026-128242	actix-http before 3.20.1 and actix-web before 4.18.2 contain an unbounded decompression vulnerability in encoding::Decoder that lets remote attackers exhaust memory and CPU via compressed bodies. Attackers can send small highly compressed gzip, deflate, Brotli or zstd request bodies to Json, Form, Bytes or String extractors, or serve them to awc clients, causing denial of service.	7.5	More Details
CVE-2026-126543	WWBN AVideo through 29.7.1 contains an improper payment verification vulnerability in plugin/PayPalYPT/ipnV2.php that credits wallets from PayPal IPNs not bound to the site's merchant account. Unauthenticated attackers can forward genuine VERIFIED recurring-payment IPNs from their own PayPal account with a chosen users_id to add wallet balance each billing cycle.	7.5	More Details
CVE-2026-52790	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, there is a library-level memory safety issue that is reachable from an unmodified official sample server (apps/server-basic/main.c) over BACnet/IP resulting in a stack-use-after-return in writable Device string properties. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	7.5	More Details
CVE-2026-91141	A vulnerability in the default configuration of vsomeip allows a remote, unauthenticated attacker to trigger massive memory allocations by sending a small TCP packet with a large, attacker-declared SOME/IP length field. This can lead to immediate service termination via OOM-kill on memory-constrained systems or total host memory exhaustion through repeated connections.	7.5	More Details
CVE-2026-126307	Nezha Dashboard before 2.6.0 contains multiple authorization, tenant isolation, and resource exhaustion vulnerabilities that allow members or unauthenticated attackers to abuse NAT, DDNS, OAuth, cron, and server transfer features. Attackers can claim undeclared Dashboard hostnames to capture login bodies, hijack DDNS profiles, create executable schedules without exec scope, or exhaust memory via buffered NAT requests.	7.5	More Details

CVE-2026-82663	The Give - Peer-to-Peer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.9.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers who know or discover an existing campaign and team ID to modify the team's name, story, goal, access and notification settings, set its profile image URL, and upload WordPress-allowed media files as parentless attachments. This vulnerability can be combined with CVE-2026-82568 to achieve unauthenticated remote code execution.	7.5	More Details
CVE-2026-91150	A flaw was found in Cockpit. This vulnerability allows a remote attacker, without prior authentication, to send specially crafted fragmented WebSocket messages. These messages accumulate without a total-size limit, leading to unbounded memory exhaustion and a denial of service in the `cockpit-ws` service.	7.5	More Details
CVE-2026-126304	NLTK from 3.10.0 before 3.10.4 contains a symlink escape vulnerability in YCOECorpusReader that allows attackers to read files outside the corpus root by planting psd or pos directory symlinks. Attackers controlling a YCOE corpus can make parsed_sents() and tagged_words() return file content from other corpora or temporary files within the NLTK data sandbox.	7.5	More Details
CVE-2026-91891	Dell Terraform Provider for PowerStore, versions prior to 1.3.1 , contains a vulnerability that may cause sensitive authentication data to be insufficiently redacted in diagnostic logs. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	7.5	More Details
CVE-2026-82568	The Give - Peer-to-Peer plugin for WordPress is vulnerable to time-based SQL Injection via the 'sort' parameter in all versions up to, and including, 2.9.3 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. Successful exploitation requires the existence of at least one Peer-to-Peer campaign. This vulnerability can be combined with CVE-2026-82663 to achieve unauthenticated remote code execution.	7.5	More Details
CVE-2026-126769	OpsTree REMS through 1.0.0 contains a missing authentication vulnerability that allows unauthenticated remote attackers to access Governance API endpoints, including /api/v1/databases. Attackers can send requests without an Authorization header, or with invalid or tampered JWT tokens, to retrieve stored database hosts, usernames, and passwords.	7.5	More Details
CVE-2026-126303	NLTK before 3.10.4 contains an uncontrolled resource consumption vulnerability in SteppingRecursiveDescentParser.parse() that lacks any max_time deadline or step limit. Attackers influencing the grammar can supply an ambiguous self-embedding grammar and short token input to force unbounded top-down search, pinning CPU cores and exhausting worker pools.	7.5	More Details
CVE-2026-126151	A incorrect implementation of authentication algorithm vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated remote attacker to gain elevation of privilege (account takeover) via a crafted request.	7.5	More Details
CVE-2026-128081	AutoMapper is a convention-based object-object mapper in .NET. Prior to 15.1.4 and from 16.0.0 until 16.3.0, AutoMapper can recurse without an effective MaxDepth limit when mapping polymorphic graphs through Include or IncludeBase, runtime-typed object or interface members, nested Dictionary<string, object> or ExpandoObject sources, or recursive ConvertUsing type converters. Deep attacker-influenced graphs on these paths can throw an uncatchable StackOverflowException and terminate the process. This issue is fixed in versions 15.1.4 and 16.3.0.	7.5	More Details
CVE-2026-126154	A out-of-bounds write vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow a remote unauthenticated attacker to cause a denial of service via a specially crafted HTTP request.	7.5	More Details
CVE-2026-123696	The Security For WooCommerce WordPress plugin through 1.0.16 does not check that the requester is authorised before resetting two-factor authentication enrolment, allowing unauthenticated users to remove the second factor from any account, or from every account at once.	7.5	More Details
CVE-2026-126609	Progressive Robot hMailServer 6.2.25 through 6.3.7 on Windows, with a PostgreSQL database, the connection's sslmode require, verify-ca or verify-full, and a root certificate file named by PostgreSQLSslRootCert (from 6.2.25) or, with TlsMode=verify-full and neither PostgreSQL key set, by TlsCaFile (from 6.3.4), hands the file's name to libpq as bytes in the system's ANSI code page (up to 6.3.5 as Latin-1 bytes, which on code page 1252 are the code page's own for U+00A0 to U+00FF), and libpq looks for the file by those bytes and then hands the same bytes to OpenSSL, whose file opening on Windows reads a name as UTF-8 first and opens the file at that reading when one is there. When every byte of the name outside ASCII also reads as UTF-8 - for example U+00C3 U+00A9, the bytes C3 A9 on code page 1252, which are U+00E9 in UTF-8 - the database server's certificate was checked against the file at that other name whenever one was there, which allows a local attacker who can create that file but cannot change the configured one, as any user can by default beside a file an administrator keeps under ProgramData, or beside a folder directly under the system drive's root whose permissions the administrator restricted, and who can intercept the connection to the database server or stand in for it, to have hMailServer trust a certificate authority of the attacker's own and read and modify the traffic between hMailServer and its database, the database password included; the file alone, holding no authority that issued the database server's certificate, stops hMailServer from connecting to its database. The same applies in 6.3.4 through 6.3.7 to TlsCaFile when an Oracle MySQL client library has been put in place of the bundled MariaDB Connector/C, since that client opens the file through OpenSSL in the same way; the bundled MariaDB	7.5	More Details

	Connector/C opens the file in the code page and is not affected, and neither are the Linux builds. The configuration is not the default: by default no root certificate file is named.		
CVE-2026-125823	Allocation of Resources Without Limits or Throttling vulnerability in Jegstudio Gutenverse gutenverse allows HTTP DoS.This issue affects Gutenverse: from n/a through 4.2.2.	7.5	More Details
CVE-2026-128344	ExcelJS through 4.4.0 contains a memory exhaustion vulnerability that allows attackers to crash applications by supplying a workbook with an unbounded image anchor column in the drawing part. Attackers can set an anchor column such as 300000000 in xl/drawings/drawing1.xml so reading getImages() anchor positions makes Worksheet.getColumn allocate millions of Column objects and abort with a heap out-of-memory error.	7.5	More Details
CVE-2026-128343	exceljs through 4.4.0 contains a denial of service vulnerability that allows attackers to block the event loop by supplying unbounded row r attributes parsed in row-xform.js. Attackers can craft an XLSX file with a row numbered far beyond Excel's limit, making getSheetValues(), workbook writes and CSV export consume time proportional to that number.	7.5	More Details
CVE-2026-123628	IBM webMethods Integration Server 10.15 and 11.1 could allow a remote attacker to obtain sensitive information due to an exposure of sensitive server-side environment variables and Java runtime details.	7.5	More Details
CVE-2026-128342	ExcelJS through 4.4.0 contains a denial of service vulnerability that allows attackers to block the event loop by supplying an unbounded sheetId in xl/workbook.xml. Attackers can provide a workbook with a huge sheetId, making the sparse worksheet array walk stall worksheets, getWorksheet and writeBuffer for seconds.	7.5	More Details
CVE-2026-109158	IBM App Connect Operator and IBM App Connect Enterprise Certified Containers Operands may allow the AI Agent to log sensitive information about the deployed environment within error messages.	7.5	More Details
CVE-2026-110951	Weak Password Recovery Mechanism for Forgotten Password vulnerability in Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure, Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure - dealer integration, and Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure - Storefront application and management panel allows Password Recovery Exploitation. This issue affects Hyper E-Commerce Infrastructure: before 1.1; Hyper E-Commerce Infrastructure - dealer integration: before 1.2; Hyper E-Commerce Infrastructure - Storefront application and management panel: before 2.1796.	7.5	More Details
CVE-2026-126277	NocoDB before 2026.08.1 contains an uncontrolled resource consumption vulnerability that allows unauthenticated attackers to exhaust server resources by sending unbounded filter arrays to shared-view bulk endpoints. Attackers with a shared view UUID can POST a large body of minimal filter objects, triggering a full database query per entry, to crash the NocoDB process.	7.5	More Details
CVE-2026-126165	A memory allocation with excessive size value vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow a remote unauthenticated attacker to cause a denial of service via a specially crafted attachment delivered over SMTP.	7.5	More Details
CVE-2026-127056	PapaParse before 5.7.1 contains an inefficient algorithmic complexity vulnerability that allows remote unauthenticated attackers to cause denial of service by submitting delimiter-free quoted CSV input to Papa.parse(). Attackers can supply a single-column quoted CSV with no delimiters, triggering repeated full-buffer indexOf scans per row that grow quadratically with input size, exhausting CPU and blocking the Node.js event loop or freezing a browser tab.	7.5	More Details
CVE-2026-126161	A uncontrolled resource consumption vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8 may allow a remote unauthenticated attacker to cause a denial of service via repeated unauthenticated POST requests.	7.5	More Details
CVE-2026-123697	The Security For WooCommerce WordPress plugin through 1.0.16 does not restrict who can request a user's current two-factor code or two-factor secret, allowing unauthenticated users to obtain them for any account and bypass the second factor on sites where its one-time password library is available.	7.5	More Details
CVE-2026-126159	A authorization bypass through user-controlled key vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an unauthenticated attacker to release or delete quarantined messages for arbitrary mailboxes via a crafted quarantine release request.	7.5	More Details
CVE-2026-123700	The Security For WooCommerce WordPress plugin through 1.0.16 does not check that the requester is authorised before running several of its comment cleanup actions, allowing unauthenticated users to permanently delete all comments on the site, including approved ones and WooCommerce order notes.	7.5	More Details
CVE-2026-127131	SOGo before 5.12.13 contains a missing rate limiting vulnerability in its web login TOTP verification that allows attackers who already possess a victim's password to brute-force the second-factor code without triggering any lockout. Attackers can send repeated POST requests to /SOGo/connect with wrong verification codes at high speed since failed TOTP attempts never increment the failed-login counter and SOGoMaximumFailedLoginCount does not apply, enabling indefinite guessing across 30-second code windows to bypass two-factor authentication.	7.4	More Details

CVE-2026-126242	A incorrect authorization vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an attacker to bypass authentication and gain unauthorized access. Full impersonation however requires the attacker to obtain pre-required id and data via other means.	7.4	More Details
CVE-2026-127111	SOGo before 5.12.13 contains an improper restriction of excessive authentication attempts vulnerability that allows unauthenticated attackers to reset account passwords by repeatedly guessing secret-question answers via the passwordRecoveryCheck endpoint without lockout or rate limiting. Attackers can submit unlimited candidate answers to obtain a valid recovery JWT, then use it to change the account password without the old credential and log in via the connect endpoint, achieving full account takeover on accounts without TOTP enabled.	7.4	More Details
CVE-2026-126280	NocoDB before 2026.08.0 contains a race condition in refresh-token rotation that allows attackers to reuse tokens because UserRefreshToken.ts never checks the affected-row count. Attackers holding a captured refresh token can present it concurrently with the legitimate user to obtain a valid authenticated session, and no reuse event is recorded.	7.4	More Details
CVE-2026-111435	Relative path traversal vulnerability in openEuler iSulad on Linux. This vulnerability is associated with program file src/daemon/modules/image/oci/oci_load.c. This issue affects iSulad: through 2.1.6. In oci_load.c, oci_load_process_manifest() does not sanitize the Config path of manifest.json. A malicious tar package can enable the isulad with the root permission to read any file on the host.	7.4	More Details
CVE-2026-64668	pam_usb provides hardware authentication for Linux using removable media. From version 0.8.0 to before version 0.9.3, the deny_remote feature in pam_usb uses /usr/bin/w -i to detect whether the authenticating user has an active remote tmux session. In pusb_tmux_has_remote_clients() (src/tmux.c), the IPv6 detection pattern matched the address group and then immediately expected whitespace. On Linux systems with multi-homed network interfaces, w -i appends a zone index (scope identifier) to link-local IPv6 addresses — e.g. fe80::1%eth0. The %eth0 suffix appeared between the address and the next whitespace field, causing the regex match to fail even for an otherwise-matching remote session. The function returned "no remote clients" and granted access. This issue has been patched in version 0.9.3.	7.4	More Details
CVE-2026-126837	A validation flaw in the DNS SRV host discovery of the MongoDB Node.js driver may cause the driver to connect to a host outside the expected domain. For a mongodb+srv:// connection string, the driver checks each host name in the DNS SRV response against the domain of the connection string. The driver then builds the connection address from the original name, in which certain characters end the host name early. An unauthenticated party who can forge or change the DNS SRV response may redirect the connection to a host of their choice. TLS does not prevent this, because the driver verifies the server certificate against the redirected host name. This may result in unintended disclosure of application data and authentication credentials, and in altered query results. Applications that use mongodb:// connection strings are not affected.	7.4	More Details
CVE-2026-91870	Dell Ansible Storage for PowerFlex, versions prior to 3.2.0, contains an Improper Certificate Validation vulnerability in the API client component. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	7.4	More Details
CVE-2026-129161	Dromara free-fs 2.0.1 through 2.3.1 contains an improper restriction of authentication attempts vulnerability that allows unauthenticated attackers to brute-force six-digit password reset codes via PUT /apis/user/forget-password. Attackers can request a code for a known email and submit unlimited guesses during its 300-second lifetime to set a chosen password and take over the account.	7.4	More Details
CVE-2026-64669	pam_usb provides hardware authentication for Linux using removable media. From version 0.8.0 to before version 0.9.3, the deny_remote feature in pam_usb uses /usr/bin/w -i to detect whether the authenticating user has an active remote tmux session. In pusb_tmux_has_remote_clients() (src/tmux.c), the IPv6 detection regex required exactly four explicit colon-separated groups of 1-4 hex digits (e.g. 2001:0db8:85a3:0000). Any IPv6 address in compressed notation — including loopback (::1), link-local (fe80::1), and global unicast addresses (2001:db8::1) — did not match this pattern. As a result the remote-client check silently returned "no remote clients" even when a remote tmux client was connected from such an address. This issue has been patched in version 0.9.3.	7.4	More Details
CVE-2026-126256	A out-of-bounds read vulnerability in Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiOS 7.0 all versions may allow an unauthenticated attacker to execute arbitrary code or command via crafted packets.	7.4	More Details
CVE-2026-128333	listmonk 6.0.0 before 7.0.0-beta.2 contains an authentication bypass vulnerability in doResetPassword that skips TOTP verification after a password reset. Attackers who can complete a reset, such as by reading the victim's reset email, obtain fully authenticated sessions including Super Admin without the TOTP code.	7.4	More Details
CVE-2026-128332	Listmonk 6.0.0 before 7.0.0-beta.2 contains a 2FA bypass vulnerability that allows attackers with a valid password to brute-force TOTP codes because the attempt counter resets on every new password login. Attackers can repeatedly submit credentials to POST /admin/login to obtain fresh tokens, each allowing 15 more guesses, gaining sessions for 2FA-protected accounts including Super Admin.	7.4	More Details
CVE-2026-128023	FrankenPHP before 1.13.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to spoof trusted headers by sending dot-form header names that PHP rewrites to underscores. Attackers can send headers like X.Authenticated.User or X.Forwarded.For that map to $_SERVER keys, spoofing user identity, client IP, or scheme.	7.4	More Details

CVE-2026-126265	SiYuan 2.1.0 before 3.8.9 contains a flaw where the loginAuth CAPTCHA challenge lives in a signed client-side cookie, allowing reuse of a solved challenge. Attackers can replay the original signed siyuan cookie with distinct wrong access codes to brute-force the code and gain an administrator session.	7.4	More Details
CVE-2026-126499	Jellyfin before 12.0 contains a path traversal vulnerability in the DELETE /Library/VirtualFolders and POST /Library/VirtualFolders/Name endpoints that allows attackers to delete or move directories via unvalidated library names. Unauthenticated attackers can supply names like .. or absolute paths before setup completes to recursively delete the data directory and jellyfin.db.	7.4	More Details
CVE-2026-126255	A path traversal: '../filedir' vulnerability in Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions may allow an unauthenticated attacker to bypass authentication via specially crafted credentials.	7.4	More Details
CVE-2026-126777	Traccar 3.15 before 6.17.0 contains an authentication bypass vulnerability in LdapProvider.login() that fails to reject empty passwords, causing LDAP binds to be performed as unauthenticated binds when LDAP authentication is enabled. Unauthenticated attackers who know a valid username can log in via POST /api/session or HTTP Basic authentication with an empty password against directories that permit unauthenticated binds, obtaining sessions for any account including administrators.	7.4	More Details
CVE-2026-126610	Progressive Robot hMailServer 6.3.4 through 6.3.7, with a MySQL or MariaDB database and TlsMode=verify-full, does not hand the database client the CA file that TlsCaFile names when the file's name contains a character outside ASCII on Linux, or above U+00FF on Windows, which allows an attacker who can intercept the connection to the database server to read and modify the traffic between hMailServer and its database, by presenting, with MariaDB Connector/C 3.4.2 to 3.4.10 as the client, a certificate from any authority, its own included, for any name, and otherwise a certificate for the database server's name issued by any certificate authority in the system's trust store. The server converted the name for the client with the C runtime's conversion in the C locale, which gives an empty string for such a name, and then set no CA file at all, without an error, while certificate verification stayed on, so the client - MariaDB Connector/C, bundled on Windows and the distribution's on Linux - verified the certificate of a database server over the network against the system's trust store instead of the configured CA; Connector/C 3.4.2 to 3.4.10 (bundled on Windows in 6.3.4 to 6.3.6) went further and, with no CA file, took a certificate within its dates whose issuer it could not find, for any name, with neither its chain nor its name checked and no password proof, when the server offered first a sign-in method that hashes the password, which an attacker in the middle chooses (MariaDB's CONC-853, fixed in Connector/C 3.4.11), and Connector/C 3.4 accepted from a MariaDB 11.4 or later server a certificate the store did not vouch for when that server proved it held the account's password; on a connection it treats as local (127.0.0.1, ::1, a Unix socket, a named pipe, and localhost on Windows), Connector/C 3.4.1 and later checked neither the certificate's issuer nor its name, so that a local attacker able to stand in for the database server could present any certificate within its dates of its own making. The settings line of hmailserver --check-database still named the configured file, and the application log said the certificate had been checked. With MariaDB Connector/C 3.4.1 to 3.4.9 as the client - bundled on Windows in 6.3.4 to 6.3.6, and the client of Linux distributions that have not patched it - the missing CA file also met the precondition of CVE-2026-107819, so that a certificate issued for any other name by a trusted authority was enough to obtain the database password. On Linux the file was found only when the server ran on glibc under a locale whose character set holds the name's characters (a UTF-8 locale, or a legacy 8-bit one the system has, in whose bytes the file is then named); with no locale, LC_ALL=C or a locale the system lacks, and on Alpine (musl), the connection failed instead. The configuration is not the default: TlsMode defaults to prefer, which checks no certificate.	7.4	More Details
CVE-2026-75494	Cudy TR3000 before 2.5.42 contains an argument injection vulnerability that allows a malicious or compromised ACS to inject curl options through unfiltered Username and Password values in the easycwmpd Upload handler. Attackers can embed whitespace to add options like -o and --url to the root-run curl command, writing attacker-controlled HTTP responses to arbitrary files on the device.	7.4	More Details
CVE-2026-123338	Out-of-bounds Write vulnerability in Apache DataSketches C++. An application that deserializes a REQ sketch from an untrusted source can have heap memory corrupted by a crafted sketch, because the serialized compactor headers were not validated. This issue affects Apache DataSketches C++: from 3.0.0 through 5.3.0. Users are recommended to upgrade to version 5.3.1, which fixes the issue.	7.4	More Details
CVE-2026-91871	Dell Ansible Storage for PowerStore, versions prior to 3.9.0, contains an Improper Certificate Validation vulnerability in the API client component. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure and unauthorized access.	7.4	More Details
CVE-2026-127079	OpsTree BuildPiper before 2.7.0 lacks rate limiting on password-reset OTP verification, allowing unauthenticated attackers to brute force 6-digit OTPs. Attackers can initiate a reset and submit unthrottled guesses to the check_otp endpoint, resetting the target's password and taking over the account.	7.4	More Details
CVE-2026-67545	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.73, the HTTP workflow node in Heym makes outbound HTTP requests to user-supplied URLs without validation of the target host or IP address. If a workflow author has already configured an HTTP node that targets internal addresses such as cloud metadata endpoints or private network hosts, and exposed the workflow with anonymous execution, an unauthenticated attacker can trigger the preconfigured SSRF sink. The same project has comprehensive SSRF protection in its MCP integration, which is absent from the HTTP node. This issue has	7.4	More Details

	been patched in version 0.0.73.		
CVE-2026-123274	Out-of-bounds Write vulnerability in Apache DataSketches C++. An application that deserializes a KLL sketch from an untrusted source can have heap memory corrupted by a crafted sketch, because the serialized level boundaries were not validated. This issue affects Apache DataSketches C++: 2.0.0 through 5.3.0. Users are recommended to upgrade to version 5.3.1, which fixes the issue.	7.4	More Details
CVE-2026-110278	IBM ContextForge MCP Gateway 1.0.0 through 1.1.0 could allow an attacker to replay identity propagation claims signatures or expose sensitive user identity information to third-party MCP servers due to static signature payloads and missing per-gateway configuration checks during tool invocation.	7.4	More Details
CVE-2026-77873	An improper permissions vulnerability was reported in Lenovo System Update that could allow a local authenticated user to execute code with elevated privileges.	7.3	More Details
CVE-2026-126997	A vulnerability was identified in JeecgBoot up to 3.9.6. This affects the function RestTemplate.exchange of the file org/jeecg/modules/airag/flow/c/a.class of the component flow-run Endpoint. The manipulation leads to server-side request forgery. 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.	7.3	More Details
CVE-2026-106140	In Progress® Telerik® Reporting prior to version 20.3.26.1110, a deserialization of untrusted data vulnerability in the .NET Framework report designers allows a local attacker with low privileges to execute arbitrary code in the context of the designer process when the user performs certain editing operations.	7.3	More Details
CVE-2026-129180	A flaw has been found in projectworlds Visitor Management System 1.0. This vulnerability affects the function mysqli_query of the file actionpage.php. This manipulation of the argument purpose causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-126624	Unverified ownership in the Windows installer of Progressive Robot hMailServer 6.3.7 allows a local authenticated user to run code as the mail server's service account or as an administrator when setup installs into, or upgrades, a program folder that accounts other than the administrators could write before, such as one made beforehand at the root of a drive. 6.3.7 fixed CVE-2026-107571 by giving the program folder, Bin and ControlPanel permissions that only administrators may change, but setup refused nothing that was already in them, or in the folders that hold the event script, the add-ons and the database scripts: a program, a library, a script or a settings file that another account owns, or whose own permissions let another account change it, is kept with that owner and those permissions, which the hardening of the folders does not take away. Setup then runs programs from Bin with the administrator's elevated rights, and the service, which runs as LocalSystem or as its virtual account, runs them and the event script, so that a library such an account placed in Bin is loaded in place of the system's; the account can still change the file after the installation. The default installation under Program Files is not affected.	7.3	More Details
CVE-2026-126622	Incorrect default permissions in the Windows installer of Progressive Robot hMailServer 6.3.7 allow a local authenticated user to run code as the administrator who runs setup, when the server is installed into a program folder that is already there and that accounts other than the administrators could write, such as a folder made beforehand at the root of a drive, or when such an installation is upgraded or repaired. 6.3.7 fixed CVE-2026-107571 by giving the program folder, Bin and ControlPanel permissions that only administrators may change, but for a folder that is already there it does so only at the end of setup: setup first copies the programs into Bin, which every user may still write, and runs programs from Bin with the administrator's elevated rights, registering the service among them, before that hardening, so that a library another account places in Bin meanwhile is loaded in place of the system's. A handle an account opened on such a folder while it could write it keeps that access after the hardening. The default installation under Program Files, whose folders give ordinary users read and execute only, is not affected.	7.3	More Details
CVE-2026-126305	EspoCRM before 9.3.11 and 10.x before 10.0.9 contains a stored cross-site scripting vulnerability in Knowledge Base articles that lets users with Knowledge Base create or edit access attach a JavaScript file and add a crafted link to the article body. When an administrator clicks the link, the script runs in their session and can create an administrator account with attacker-chosen credentials.	7.3	More Details
CVE-2026-127286	A vulnerability was identified in Zackriya-Solutions Meetily up to 0.4.1. Affected is an unknown function of the file backend/app/main.py. The manipulation leads to missing authentication. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The legacy backend was not removed yet. Vulnerable code is still present on main. The vendor explains: "[W]e are moving towards a single unified application using the tauri framework, and we deprecated the client-server architecture of this application."	7.3	More Details
CVE-2026-107484	An input and authorization validation vulnerability in Gaia Portal backend handlers could allow an authenticated, non-administrative user to perform privileged operations that should be restricted to administrators.	7.3	More Details
CVE-2026-127278	A weakness has been identified in AIP-PUB ACPs-community up to 2.2.0. The impacted element is the function send_verification_code of the file registry-server/app/account/service_auth.py of the component verify-code Endpoint. Executing a manipulation of the argument phone can lead to improper authentication. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The reported GitHub issue was closed with the reason "completed". However, it was not possible to determine the PR	7.3	More Details

	or commit which could have fixed this issue.		
CVE-2026-127281	A vulnerability was found in lanyulei ferry 1.0.0-beta.1/1.0.0. Affected is an unknown function of the file middleware/auth.go of the component JWT Validation. The manipulation results in improper authentication. 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.	7.3	More Details
CVE-2026-126451	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability that allows portal patients to run JavaScript in staff sessions by injecting javascript: URLs into document template_data. Attackers can submit an encounterForm value rendered unsanitized into an iframe src by DocumentTemplateRender, letting the script read PHI and CSRF tokens and call staff or admin endpoints.	7.3	More Details
CVE-2026-127284	A security flaw has been discovered in SourceCodester Food Ordering System 1.0. This affects an unknown part of the file admin/add_category.php of the component Admin Write Handler. Performing a manipulation of the argument title/description/price/current_image/featured/active/id 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.	7.3	More Details
CVE-2026-123747	A flaw was found in pappl-retrofit. The application fails to properly sanitize user-supplied filenames when handling the upload and deletion of PostScript Printer Description (PPD) files. A remote, unauthenticated attacker can exploit this directory traversal flaw by submitting filenames containing path traversal sequences. This allows the attacker to upload or delete arbitrary files on the system, which can result in data corruption, denial of service, or arbitrary command execution.	7.3	More Details
CVE-2026-129359	A security flaw has been discovered in Linux Foundation Magma up to 1.9.0. The affected element is an unknown function of the file orc8r/lib/go/registry/interceptors.go. Performing a manipulation results in hard-coded credentials. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-129360	A weakness has been identified in Linux Foundation Magma up to 1.9.0. The impacted element is an unknown function of the file orc8r/cloud/go/services/obsidian/access/operator.go of the component Obsidian REST. Executing a manipulation of the argument X-Magma-Client-Cert-Serial can lead to authentication bypass by spoofing. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-127279	A vulnerability was detected in AIP-PUB ACPs-community up to 2.2.0. This impacts an unknown function of the file discovery-server/app/main.py of the component Discovery Server. The manipulation results in missing authentication. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	7.3	More Details
CVE-2026-129181	A vulnerability has been found in projectworlds Visitor Management System 1.0. This issue affects the function mysqli_query of the file /img/user%20page.php of the component Login Endpoint. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-127283	A vulnerability was identified in SourceCodester Food Ordering System 1.0. Affected by this issue is some unknown functionality of the file admin/update_food.php of the component Admin Image Handler. Such manipulation of the argument cmd leads to unrestricted upload. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-129262	A weakness has been identified in Wuxi Wubang Security Software Wubang Five-in-One Safety Production Management Information System up to 3.5. Affected by this vulnerability is the function DiyFileUpload of the file /ws.asmx. This manipulation causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-91151	A flaw was found in Cockpit. A local authenticated user with control over a target account's home directory can exploit a privileged symlink dereference vulnerability in the `ssh-add-public-key.sh` helper. When this helper runs with elevated privileges, it can be tricked into following attacker-controlled symlinks within the `.ssh` or `authorized_keys` paths. This allows the attacker to arbitrarily change file ownership and modes, potentially leading to local privilege escalation and impacting the integrity, confidentiality, and availability of the system.	7.3	More Details
CVE-2026-127084	Teable before 2026-10-12T12-45-53Z.3331 contains a stored cross-site scripting vulnerability that allows authenticated users to upload SVG or HTML attachments with an attacker-chosen content type. Attackers can send the same-origin /api/attachments/read URL, served inline with an empty Content-Security-Policy, to run script with the victim's session and perform API actions.	7.3	More Details
CVE-2026-126795	A vulnerability was determined in ToolJet up to 3.20.256-lts/3.21.93-beta. The impacted element is the function activateUserWithPassword of the file server/src/modules/onboarding/util.service.ts of the component Onboarding Signup Endpoint. Executing a manipulation of the argument email can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 3.21.94-beta is sufficient to resolve this issue. This patch is called af8f17a745621ae418f1743440f63d315e8b8643. The affected component should be upgraded. The vendor was contacted early about this disclosure.	7.3	More Details

CVE-2026-126998	A security flaw has been discovered in JeecgBoot up to 3.9.5. This vulnerability affects the function OpenApiController.call of the file /openapi/call of the component Authentication Filter. The manipulation results in server-side request forgery. 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.	7.3	More Details
CVE-2026-120153	SQL injection in PostgreSQL extension-script substitutions allows an attacker with database-level CREATE privilege to execute arbitrary code as the bootstrap superuser, via a schema or owner name containing newlines or other special substrings. This is similar to CVE-2023-39417, but it requires a non-bundled extension with a vulnerable script pattern. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	7.2	More Details
CVE-2026-82177	Dell PowerStore contains an OS Command Injection vulnerability. A high-privileged attacker could exploit this vulnerability, potentially leading to arbitrary root command execution on the appliance.	7.2	More Details
CVE-2026-103769	Deserialization of Untrusted Data vulnerability in Acowebs PDF Invoices and Packing Slips For WooCommerce pdf-invoices-and-packing-slips-for-woocommerce allows Object Injection.This issue affects PDF Invoices and Packing Slips For WooCommerce: from n/a through 1.4.10.	7.2	More Details
CVE-2026-129101	Cudy TR3000 before 2.5.42 contains a mass assignment vulnerability in the vpn.set_conf App RPC method that allows authenticated administrators to inject arbitrary OpenVPN server options. Attackers can set enabled=1 and a malicious up option in the openvpns object, which the openvpn-hotplug wrapper executes via /bin/sh as root.	7.2	More Details
CVE-2026-129100	Cudy TR3000 before 2.5.42 contains a remote code execution vulnerability that allows authenticated administrators to execute commands as root by uploading crafted OpenVPN private or tls-auth keys. Attackers can close the inline key block with </key>, inject directives such as tls-verify that bypass the .ovpn denylist, and have OpenVPN execute the hook as root.	7.2	More Details
CVE-2026-6467	Uncontrolled search path element in PostgreSQL CREATE EXTENSION allows an attacker with database-level CREATE privilege to execute arbitrary code as the bootstrap superuser, via ALTER SCHEMA ... RENAME or CREATE EXTENSION ... SCHEMA "$user". ALTER EXTENSION was also affected. A trusted-extension script located the wrong object and executed arbitrary SQL of the attacker's choice. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	7.2	More Details
CVE-2026-129099	Cudy TR3000 before 2.5.42 contains a remote code execution vulnerability that allows authenticated administrators to run root commands by importing a malicious OpenVPN client configuration. Attackers can include tls-verify or ipchange directives, which the incomplete denylist does not filter, to execute commands as root when the router connects to an attacker-controlled VPN endpoint.	7.2	More Details
CVE-2026-107522	Dell PowerStore contains an Improper Authorization vulnerability. An authenticated user could exploit this vulnerability, potentially leading to privilege escalation to administrator.	7.2	More Details
CVE-2026-116313	Untrusted search path in PostgreSQL vacuumdb allows a database owner to execute arbitrary SQL as the database user running vacuumdb, via shadowing operators used in the --missing-stats-only catalog query. The pg_upgrade documentation recommends an affected vacuumdb invocation. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are unaffected.	7.2	More Details
CVE-2026-75785	An improper neutralization of special elements used in an OS command vulnerability in the VPN API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users with administrator privileges to read or write arbitrary files and conduct denial-of-service attacks.	7.2	More Details
CVE-2026-116753	The Multi Step for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'multipart field name (array key)' parameter in all versions up to, and including, 2.9.1 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. Successful exploitation requires the target CF7 form to have the 'Save every step' option enabled and the Database for Contact Form 7 companion plugin to be active with its 'Expandable' table option enabled, both of which are disabled by default.	7.2	More Details
CVE-2026-12427	The ARforms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'description' parameter in all versions up to, and including, 7.2.4 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. The injected payload is deserialized via maybe_unserialize() when an administrator views the affected entry; if the attacker's array contains a 'referrer' key, the attacker-controlled page_url and http_referrer values are used as-is and rendered unescaped into the admin entry detail view.	7.2	More Details
CVE-2026-120688	The EZ SQL Reports Shortcode Widget and DB Backup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'HTTP_USER_AGENT (demonstrated); more generally, any attacker-controllable DB column the saved report selects' parameter in all versions up to, and including, 5.25.25 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 saved a SQL report that selects an attacker-controllable database column, such as wp_comments.comment_agent, which WordPress stores verbatim from unauthenticated visitors even when comments are pending moderation.	7.2	More Details

CVE-2026-64671	Waline is a comment system with backend support. In versions 3.15.2 and prior, the @waline/client UserList widget builds its DOM by concatenating server-returned commenter fields directly into root.innerHTML with no HTML escaping. The commenter nick and link are stored and returned verbatim by the server (only the comment body is sanitized), and the link field is never sent to the spam filter. So an unauthenticated visitor who posts a comment with link = x"><img src=x onerror=...> achieves stored cross-site scripting that executes, with no interaction, in the browser of every visitor to a page that embeds the UserList widget. At time of publication, there are no publicly available patches.	7.2	More Details
CVE-2026-12424	The ARforms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Referer Header in all versions up to, and including, 7.2.4 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. The arf_save_incomplete_form_data() AJAX handler is registered with wp_ajax_nopriv_, meaning unauthenticated attackers can store a malicious payload by submitting a partial form entry with a forged Referer header, with no authentication required at any step.	7.2	More Details
CVE-2026-126489	OpenEMR before 8.5.0 contains a second-order SQL injection vulnerability in the IPPF contraceptive issue feature because issue_ippf_con_save concatenates layout_options field_id values into a REPLACE INTO query as column names. Authenticated administrators can add a malicious field_id via edit_layout.php, then trigger issue_ippf_con_save through add_edit_issue.php to execute arbitrary SQL.	7.2	More Details
CVE-2026-126425	OpenEMR before 8.5.0 contains a stored SQL injection vulnerability in which History layout field identifiers saved through edit_layout.php, including HIS fields and LBF source-H fields, are placed unvalidated into an INSERT statement for patients without a history_data row. Users with admin/super and patients/med write access can trigger history_save.php or LBF saves to execute SQL functions like SLEEP, tying up database workers or accessing data beyond their privileges.	7.2	More Details
CVE-2026-125912	The WP Ultimate CSV Importer WordPress plugin before 9.2 does not restrict the destination filename and extension, nor validate the fetched content type, when importing remote media, allowing an Administrator of a Multisite subsite to write and execute arbitrary PHP in the shared WordPress context despite not being a Network Administrator and being unable to install WP Ultimate CSV Importer WordPress plugin before 9.2 or edit files.	7.2	More Details
CVE-2026-126178	A heap-based buffer overflow vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker with admin privileges to execute unauthorized code or commands via a crafted request.	7.2	More Details
CVE-2026-126249	A improper privilege management vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an authenticated attacker to escalate privileges.	7.2	More Details
CVE-2026-126211	A improper privilege management vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.1 through 7.6.7, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.1 through 7.6.7, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.1 through 7.6.7, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.1 through 7.6.7 may allow an authenticated privileged attacker to elevate their privileges via crafted JSON-RPC request.	7.2	More Details
CVE-2026-126185	A improper control of generation of code ('code injection') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow an authenticated administrator to execute unauthorized code or commands via specially crafted requests.	7.2	More Details
CVE-2026-126182	A improper control of generation of code ('code injection') vulnerability in Fortinet FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow a remote authenticated attacker to execute unauthorized code or commands via crafted HTTP requests.	7.2	More Details
CVE-2026-62971	The OWASP core rule set (CRS) is a set of generic attack detection rules for use with compatible web application firewalls. Prior to versions 3.3.10, 4.25.1, and 4.28.0, CRS rules in the 921 (protocol-attack), 930 (LFI), 931 (RFI), 932 (RCE), 933 (PHP), 934 (generic), 941 (XSS), 942 (SQLi), and 943 (session-fixation) families inspect XML request bodies via the XPath expression XML:/*. That expression matches only element text nodes — it does not match XML attribute values. As a result, an attacker who places an attack payload inside an XML attribute (e.g. or) bypasses CRS detection entirely. This is verified empirically against a local CRS test instance and against the public CRS sandbox. The bypass affects approximately 159 rules across 9 rule files and applies at every paranoia level (PL1 through PL4), since the variable list is more or less shared across PLs. The 944 (Java) family is the only one that correctly includes XML://@* in addition to XML:/* and is therefore unaffected. This issue has been patched in versions	7.2	More Details

	3.3.10, 4.25.1, and 4.28.0.		
CVE-2026-126179	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to execute unauthorized code or commands via specially crafted requests	7.2	More Details
CVE-2026-65949	Improper neutralization of special elements used in an OS command in Lenovo XClarity Integrator for Microsoft Windows Admin Center 5.1.1 and 5.2.0 allows an authenticated remote attacker to execute arbitrary PowerShell commands by submitting a crafted hostname.	7.2	More Details
CVE-2026-126171	A use of externally-controlled format string vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker to execute unauthorized commands via specially crafted HTTP request	7.2	More Details
CVE-2026-126243	A incorrect authorization vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an attacker to bypass authentication and gain unauthorized access. Full impersonation however requires the attacker to obtain pre-required id and data via other means.	7.2	More Details
CVE-2026-126169	A improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.2, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an authenticated remote attacker with domain admin or admin privileges to delete users of other tenant domains on a paired FortiAuthenticator, execute arbitrary code as root or arbitrary CLI commands, and read or write arbitrary files as root via crafted HTTP requests to the administrative interface.	7.2	More Details
CVE-2026-126168	A improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.2, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an authenticated remote attacker with domain admin or admin privileges to delete users of other tenant domains on a paired FortiAuthenticator, execute arbitrary code as root or arbitrary CLI commands, and read or write arbitrary files as root via crafted HTTP requests to the administrative interface.	7.2	More Details
CVE-2026-126166	A improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.2, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an authenticated remote attacker with domain admin or admin privileges to delete users of other tenant domains on a paired FortiAuthenticator, execute arbitrary code as root or arbitrary CLI commands, and read or write arbitrary files as root via crafted HTTP requests to the administrative interface.	7.2	More Details
CVE-2026-126158	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1 may allow an authenticated administrator to execute unauthorized code or commands as root via specially crafted HTTP requests.	7.2	More Details
CVE-2026-125637	A flaw was found in the Konflux UI proxy. Hostname values defined in the KonfluxUI custom resource are inserted directly into proxy configuration files without adequate validation or sanitization. An authenticated user with permissions to modify the custom resource can inject malicious configuration directives to bypass authentication and authorization controls, potentially exposing internal backend services. In addition, providing malformed input can cause the configuration generator to fail, resulting in a denial of service (DoS) by preventing the proxy from starting.	7.2	More Details
CVE-2026-126146	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.4, FortiMail 7.4.0 through 7.4.6, FortiMail 7.2.0 through 7.2.9, FortiRecorder 7.6.0, FortiRecorder 7.2.0 through 7.2.11, FortiRecorder 7.0.0 through 7.0.6 may allow an authenticated privileged attacker to execute unauthorized code or commands via a specifically crafted archive account configuration.	7.2	More Details
CVE-2026-126145	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all versions may allow an authenticated administrator with system-time read-write access to execute unauthorized code or commands as root.	7.2	More Details
CVE-2026-126247	A use of externally-controlled format string vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an authenticated privileged attacker to execute unauthorized code or commands via http requests.	7.2	More Details
CVE-	A heap-based buffer overflow vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0 through 8.0.1, FortiManager		More

2026-126212	7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow an authenticated administrator to execute unauthorized code or commands or cause a denial of service via specially crafted JSON-RPC requests.	7.2	Details
CVE-2026-124008	XWEB EVO 5.2.3 through 5.8.8 contains an authenticated OS command injection vulnerability in the devices.lua template handling, which allows authenticated attackers to execute arbitrary commands by injecting unescaped template source into unzip and related shell commands. Attackers can exploit this flaw through the wlua interpreter to execute arbitrary commands with root privileges on the affected device. This product line reached it's end of service date in March 2026.	7.2	More Details
CVE-2026-126221	A improper neutralization of special elements in output used by a downstream component ('injection') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow an authenticated administrator to read or write arbitrary files or execute unauthorized code or commands via specially crafted requests to the GUI.	7.2	More Details
CVE-2026-126223	A stack-based buffer overflow vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow an authenticated administrator to execute unauthorized code or commands or cause a denial of service via specially crafted JSON-RPC requests.	7.2	More Details
CVE-2026-126224	A improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated privileged admin user to execute unauthorized code or commands.	7.2	More Details
CVE-2026-126226	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated privileged attacker to execute unauthorized code or commands via crafted report schedule name.	7.2	More Details
CVE-2026-126227	A unintended proxy or intermediary ('confused deputy') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker to execute commands outside of the intended scope via specially crafted HTTP request	7.2	More Details
CVE-2026-126228	A out-of-bounds write vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.4 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.4 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.4 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.4 through 7.2.12 may allow an authenticated remote attacker with admin privileges to execute unauthorized code or commands via a specially crafted request.	7.2	More Details
CVE-2026-126222	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.3 through 7.6.7, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.3 through 7.6.7, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.3 through 7.6.7, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.3 through 7.6.7 may allow an authenticated attacker with admin privileges to execute unauthorized code or commands via crafted requests.	7.2	More Details
CVE-2026-126230	A use of externally-controlled format string vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to execute unauthorized code or	7.2	More Details

	commands or cause a denial of service via specially crafted requests.		
CVE-2026-126220	A improper neutralization of special elements in output used by a downstream component ('injection') vulnerability in Fortinet FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11 may allow an authenticated administrator to read or write arbitrary files or execute unauthorized code or commands via specially crafted requests to the GUI.	7.2	More Details
CVE-2026-126236	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker to execute unauthorized code or commands via specially crafted HTTP requests	7.2	More Details
CVE-2026-126231	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2 all versions, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2 all versions, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2 all versions may allow an authenticated attacker to execute unauthorized commands via a crafted HTTP request.	7.2	More Details
CVE-2026-126219	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer Cloud 8.0.0, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager Cloud 8.0.0, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11 may allow an authenticated administrator to read or write arbitrary files or execute unauthorized code or commands via specially crafted requests to the GUI.	7.2	More Details
CVE-2026-126233	A unrestricted upload of file with dangerous type vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to upload arbitrary files via specially crafted requests.	7.2	More Details
CVE-2026-125771	Incorrect Privilege Assignment vulnerability in AtlasAiDev MCP Server for WordPress ai-workflow-automation-ai-agent-hub allows Privilege Escalation.This issue affects MCP Server for WordPress: from n/a through 2.0.3.	7.2	More Details
CVE-2026-126214	A authentication bypass by spoofing vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12 may allow an authenticated administrator to escalate their privileges, bypass authorization controls or impersonate internal services via specially crafted requests to the GUI.	7.2	More Details
CVE-2026-126234	A improper neutralization of special elements used in a template engine vulnerability in Fortinet FortiAnalyzer 8.0.0, FortiAnalyzer Cloud 8.0.0, FortiManager 8.0.0, FortiManager Cloud 8.0.0 may allow an authenticated attacker with restricted privileges to execute unauthorized code or commands via a specially crafted request.	7.2	More Details
CVE-2026-126235	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.2 through 7.6.7, FortiAnalyzer 7.4.7 through 7.4.11, FortiAnalyzer 7.2.10 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.2 through 7.6.7, FortiManager 7.4.7 through 7.4.11, FortiManager 7.2.10 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to write arbitrary files via a specially crafted archive.	7.2	More Details
CVE-2026-124009	XWEB EVO 5.2.3 through 5.8.8 contains an authenticated OS command injection vulnerability that allows authenticated attackers to execute arbitrary commands as root by injecting shell metacharacters into the output device path parameter processed by backup.lua. Attackers can exploit the unescaped concatenation into mount, unzip, and related shell commands run via the wlua interpreter, including through the setuid xwbackup.cgi and xwrestore.cgi interfaces, to achieve full system compromise. This product line reached it's end of service date in March 2026.	7.2	More Details
CVE-	A improper neutralization of special elements used in a command ('command injection') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.2, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2 all		

2026-126167	versions may allow an authenticated remote attacker with domain admin or admin privileges to delete users of other tenant domains on a paired FortiAuthenticator, execute arbitrary code as root or arbitrary CLI commands, and read or write arbitrary files as root via crafted HTTP requests to the administrative interface.	7.2	More Details
CVE-2026-126803	Rote through 2.6.0 contains a privilege escalation vulnerability that allows authenticated admins to obtain super_admin rights by reading or overwriting JWT signing secrets via /v2/api/admin/settings. Attackers can retrieve the unmasked jwtSecret from the security settings group and forge HS256 tokens for the super administrator to change user roles and escalate their own account.	7.2	More Details
CVE-2026-126780	Webmin through 2.670 contains a privilege escalation vulnerability in acl/save_group.cgi that allows delegated administrators to grant unauthorized modules by submitting arbitrary module lists in the mod parameter. Attackers with Webmin Users module access can create or edit groups holding modules like Command Shell and assign themselves membership to execute commands as root.	7.2	More Details
CVE-2026-129103	Cudy TR3000 before 2.5.42 contains a command injection vulnerability that allows authenticated administrators to execute commands as root by injecting newlines into reboot_time. Attackers can submit a reboot_time value followed by a newline and crontab line, which /etc/init.d/autoreboot writes to the root crontab for crond to run.	7.2	More Details
CVE-2026-75578	Cudy TR3000 before 2.5.42 contains a command injection vulnerability in luci/model/cbi/vpn/openvpn/client.lua, which embeds the shellquote()-quoted remote host token of an uploaded OpenVPN configuration inside an already single-quoted sed program run by os.execute(), so the nested quotes terminate the outer quote. Authenticated administrators can upload an .ovpn file whose remote host token contains a semicolon to execute arbitrary commands as root.	7.2	More Details
CVE-2026-75487	Cudy TR3000 before 2.5.42 contains a command injection vulnerability that allows authenticated administrators to execute commands as root via the WireGuard server private_key option. Attackers can save a private key containing $() command substitution, which runs when action_wireguards_export() passes it to luci.sys.exec during configuration export.	7.2	More Details
CVE-2026-120687	The Lightbox & Modal Popup WordPress Plugin – FooBox plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'img alt attribute inside .wp-caption container' parameter in all versions up to, and including, 2.8.7 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 by Subscriber-level users when bbPress is installed, as its bbp_filter_kses filter chain permits img and pre tags while preserving numeric character references inside attribute values, allowing encoded payloads to bypass save-time sanitization and reach the vulnerable sink fully intact. Exploitation by attackers with subscriber-level access and above requires that bbPress 2.6.20 is installed, a public forum exists, and either the first topic has already been approved or subsequent topics clear moderation. On a default installation, where that is not configured, the vulnerability requires attackers with contributor-level access and above.	7.2	More Details
CVE-2026-75577	Cudy TR3000 before 2.5.42 contains a command injection vulnerability that allows authenticated administrators to execute commands as root by storing a malicious WireGuard private key. Attackers can save a private_key containing $() shell substitution and call the vpn.export_conf method on the /cgi-bin/luci/rpc/app JSON-RPC endpoint, which passes the key to a wg pubkey shell command.	7.2	More Details
CVE-2026-75576	Cudy TR3000 before 2.5.42 contains a command injection vulnerability that allows authenticated administrators to execute commands as root via an unvalidated multipart filename in the CBI FileUpload handler. Attackers can upload a valid OpenVPN configuration file through the VPN client config page with a filename containing $() shell substitution, which is passed through Lua %q to /bin/sh -c.	7.2	More Details
CVE-2026-126402	Fleet before 4.89.0 contains an incorrect authorization flaw in its user administration API that accepts user creation or modification when the caller administers any one of the assigned teams. Authenticated team administrators can grant users administrator roles on other teams, then deploy software and execute scripts on those teams' hosts.	7.2	More Details
CVE-2026-76079	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Prior to version 0.224.0, an organization ADMIN can mint an OWNER membership via createUser, bypassing the owner-only set-owner authorization gate. This issue has been patched in version 0.224.0.	7.2	More Details
CVE-2026-129102	Cudy TR3000 before 2.5.42 contains a command injection vulnerability that allows authenticated administrators to execute commands as root by injecting newlines into the IPsec keyexchange field of the vpn.set_conf RPC method. Attackers can append a second leftupdown directive to ipsec.conf, which StrongSwan's updown plugin runs as root when an attacker-controlled peer establishes the CHILD_SA.	7.2	More Details
CVE-2026-126805	WWBN AVideo through 29.7.1 contains an incorrect authorization vulnerability that allows delegated Videos Admin users to obtain video_id_hash values bound to any video owner via encoder endpoints like aVideoEncoderStatus.json.php. Attackers can request the hash for an administrator-owned video and replay it through useVideoHashOrLogin() for password-less login, gaining plugin upload, configuration, and user management access.	7.2	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in madalin.ungureanu Custom Post Types and Custom Fields creator – WCK wck-custom-fields-and-custom-post-	7.1	More

125783	types-creator allows Reflected XSS.This issue affects Custom Post Types and Custom Fields creator – WCK: from n/a through 2.4.0.		Details
CVE-2026-124698	In Progress Kendo UI for jQuery, the Chart default tooltip renders point values as raw HTML. An attacker who can influence a string point value can inject markup that executes as JavaScript when a user hovers over the point. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. Version 2016.2.607 or earlier may be affected, but earlier releases have not been verified. The latest vulnerable version is 2026.3.1015; the issue is fixed in version 2026.4.1111.	7.1	More Details
CVE-2026-64666	pam_usb provides hardware authentication for Linux using removable media. Prior to version 0.9.3, src/local.c reads XRDP_SESSION with plain getenv(3) at the head of pusb_local_login while every other env consumer in the same function uses secure_getenv(3). When pam_usb.so loads into a setuid PAM host, the calling user controls the environment passed in. Clearing XRDP_SESSION before invoking the host bypasses the explicit XRDP-deny rule. Other remote-detection signals (rmsvc, evdev, loginctl, utmp) may still catch the session, but the env-based detection alone is defeated. This issue has been patched in version 0.9.3.	7.1	More Details
CVE-2026-126213	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated attacker to execute unauthorized SQL commands via specially crafted requests.	7.1	More Details
CVE-2026-125452	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Denishua WPJAM Basic wpjam-basic allows Reflected XSS.This issue affects WPJAM Basic: from n/a through 7.1.2.	7.1	More Details
CVE-2026-124259	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Franky Events Made Easy events-made-easy allows Reflected XSS.This issue affects Events Made Easy: from n/a through 3.3.5.	7.1	More Details
CVE-2026-125765	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShortPixel ShortPixel Adaptive Images shortpixel-adaptive-images allows Stored XSS.This issue affects ShortPixel Adaptive Images: from n/a through 3.11.6.	7.1	More Details
CVE-2026-124697	In Progress Kendo UI for jQuery, Chart shared-tooltip rendering treats bound category and series-name values as raw HTML. An attacker who can influence values consumed by an affected Chart can inject markup that executes as JavaScript when a user displays the shared tooltip. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. Version 2016.2.607 or earlier may be affected, but earlier releases have not been verified. The latest vulnerable version is 2026.3.1015; the issue is fixed in version 2026.4.1111.	7.1	More Details
CVE-2026-125733	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DevItems ShopLentor woolentor-addons allows Reflected XSS.This issue affects ShopLentor: from n/a through 3.5.7.	7.1	More Details
CVE-2026-124018	Gutenverse Form plugin for WordPress before 3.2.2 contains a CSV formula injection vulnerability that allows unauthenticated attackers to inject spreadsheet formula-trigger characters by submitting free-text field values to the public form-submit REST route, which sanitizes input with sanitize_text_field() without stripping characters such as =, +, @, or a leading minus. Attackers can store malicious formulas in entry-data post meta that are later exported unneutralized via fputcsv() or esc_html() in the CSV export functions, causing the formula to execute when an administrator opens the exported file, enabling data exfiltration to an attacker-controlled URL or command execution on the administrator's workstation.	7.1	More Details
CVE-2026-126566	Semantic MediaWiki 7.3.1 before 7.4.1 contains an incorrect authorization vulnerability in EditProtectionUpdater::userMayChangeProtection() that checks protection changes against the page's latest revision author. Editors can add {{#set:Is edit protected=false}} to a transcluded template, removing administrator edit and move protection logged under the administrator's name.	7.1	More Details
CVE-2026-125793	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in flexmls Flexmls® IDX flexmls-idx allows Reflected XSS.This issue affects Flexmls® IDX: from n/a through 4.1.2.	7.1	More Details
CVE-2026-65967	Fider is a feedback portal for feature requests and suggestions. Prior to version 0.34.0, a Server-Side Request Forgery (SSRF) vulnerability exists in Fider due to insufficient validation of webhook URLs. The application allows user-controlled URLs to be fetched by the server without restricting access to internal or external network resources. This enables attackers with administrative privileges to make arbitrary HTTP requests from the server, potentially accessing internal services or cloud metadata endpoints. This issue has been patched in version 0.34.0.	7.1	More Details
CVE-	In Progress Kendo UI for jQuery, Spreadsheet sheet names are inserted into the SheetsBar menu button's data-sheet-name attribute without encoding. An attacker who can influence a sheet name can inject an event-handler		

2026-124696	attribute and execute JavaScript when a user hovers over the menu button. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected version is 2024.4.1112; the latest vulnerable version is 2026.3.1015. The issue is fixed in version 2026.4.1111.	7.1	More Details
CVE-2026-126309	OpenBao before 2.6.5 and 2.7.2 contains a path traversal vulnerability in Transit key import that allows authenticated attackers to bypass name restrictions in ACL policies. Attackers limited by a required_parameters name constraint can craft traversal sequences during import to write key material under arbitrary Transit key names.	7.1	More Details
CVE-2026-124969	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the replace_urls_in_value function in all versions up to, and including, 4.2.19. 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). Successful exploitation requires PEAR's Archive_Tar library to be present and loadable on the host (common in official WordPress Docker images and many PHP distributions), and an administrator must subsequently use the plugin's Rename control on any attachment after the attacker has staged a malicious payload in a comment. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	7.1	More Details
CVE-2026-126561	Semantic MediaWiki 2.5.0 before 7.4.1 contains a missing authorization vulnerability that allows editors without the edit-protection right to lock pages by adding an Is edit protected annotation. Attackers can add [[Is edit protected::true]] to pages or #set it in widely transcluded templates, so the TitleQuickPermissions hook blocks other editors and administrators from editing, moving or deleting them indefinitely.	7.1	More Details
CVE-2026-126312	OpenBao before 2.6.5 and 2.7.x before 2.7.2, and the openbao-plugins LDAP and RADIUS auth plugins before 0.2.0, contain an ACL bypass in the AppRole, Cert, LDAP, and RADIUS auth methods caused by implicit path canonicalization. Authenticated attackers can request non-canonical paths for AppRole Role IDs, Cert CRLs, LDAP groups and users, or RADIUS users to evade ACL deny rules.	7.1	More Details
CVE-2026-124254	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Exactly WWW LLC EWWW Image Optimizer ewww-image-optimizer allows Stored XSS.This issue affects EWWW Image Optimizer: from n/a through 8.9.1.	7.1	More Details
CVE-2026-126492	OpenEMR before 8.5.0 contains a second-order sql injection vulnerability that allows low-privileged authenticated users to store malicious SQL via library/ajax/addlistitem.php. Attackers can persist a SQL fragment in the recent_patient_columns option_id value, which dynamic_finder.php concatenates into a SELECT query and executes as SQL.	7.1	More Details
CVE-2026-110987	The RegistrationMagic WordPress plugin before 6.1.0.4 does not properly escape a user-supplied value before printing it inside an inline script block on several of its admin screens, allowing unauthenticated attackers to inject arbitrary JavaScript that executes in the session of an administrator who is tricked into opening a crafted link.	7.1	More Details
CVE-2026-124695	In Progress Kendo UI for jQuery Form, the items[].hint option is documented as a string but is rendered as HTML. An attacker who can influence a Form item's hint can cause attacker-controlled markup to execute as JavaScript when a user views the rendered form. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected version is 2020.2.513; the latest vulnerable version is 2026.3.1015. The issue is fixed in version 2026.4.1111.	7.1	More Details
CVE-2026-124270	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 9.3.3.	7.1	More Details
CVE-2026-125813	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Survey Maker survey-maker allows Reflected XSS.This issue affects Survey Maker: from n/a through 5.2.4.3.	7.1	More Details
CVE-2026-125828	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP BookIt bookit allows Stored XSS.This issue affects BookIt: from n/a through 2.6.0.7.	7.1	More Details
CVE-2026-52786	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, in the official apps/epics client tool on v1.6.0-rc1 (not in the generic BACnet RPM ACK decoder alone) a malicious BACnet/IP endpoint can reply to the EPICS tool’s legitimate ReadPropertyMultiple request with a syntactically valid ReadPropertyMultiple-ACK that contains more heading properties than the tool’s fixed local storage can hold. The response is decoded successfully and later consumed by ProcessRPMData(), which writes property values into a fixed global array using an unbounded linear index. This results in a reproducible global-buffer-overflow in apps/epics/main.c. This is a network-reachable memory corruption in the official epics tool’s response-processing path. The root cause is that apps/epics treats a remotely supplied variable-length RPM property list as if it were a trusted, fixed-size local heading-property set. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	7.1	More Details
CVE-	The Knowledge Building WordPress plugin before 0.7.3 does not escape several user-supplied values before		More

2026-121863	echoing them back in the response of an AJAX action available to unauthenticated users, and serves that response as HTML, leading to a Reflected Cross-Site Scripting.	7.1	Details
CVE-2026-119517	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Catna – Woo Name Your Price and Offers catna-woo-name-your-price-and-offers allows Reflected XSS.This issue affects Catna – Woo Name Your Price and Offers: from n/a through 2.0.3.	7.1	More Details
CVE-2026-126809	WWBN AVideo through 29.7.1 contains a missing authorization vulnerability in objects/import.json.php that allows uploaders to import other users' MP4 files by referencing any folder under videos/. Attackers can copy private, unlisted, password-protected or pay-per-view videos, read victims' .txt/.html sidecars as descriptions, list files via objects/listFiles.json.php, and delete victims' media using the delete parameter.	7.1	More Details
CVE-2026-125791	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iWorks Orphans sierotki allows Stored XSS.This issue affects Orphans: from n/a through 3.4.6.	7.1	More Details
CVE-2026-125790	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows Stored XSS.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.20.	7.1	More Details
CVE-2026-126416	OpenEMR before 8.5.0 contains an improper authorization vulnerability in patient_tracker_status.php that allows low-privilege authenticated users to modify other patients' tracker entries by supplying arbitrary tracker_id values. Attackers can post statustype and roomnum parameters with a valid CSRF token to alter patient-flow status, room assignments, and linked calendar appointment state.	7.1	More Details
CVE-2026-124260	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jacob N. Breetvelt WP Photo Album Plus wp-photo-album-plus allows Reflected XSS.This issue affects WP Photo Album Plus: from n/a through 9.3.06.001.	7.1	More Details
CVE-2026-126494	OpenEMR before 8.4.0 contains an improper authorization vulnerability in ScopeRepository::finalizeScopes() that allows read-only SMART/OAuth clients to obtain write scopes because ScopeEntity::containsScope() ignores registered permissions. Attackers with a client registered for user/<resource>.read can request user/<resource>.write to create, update, and delete appointments or patient data.	7.1	More Details
CVE-2026-125789	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows Stored XSS.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.20.	7.1	More Details
CVE-2026-111552	Use of single-factor authentication vulnerability in Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure, Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure - dealer integration, and Hyper Teknoloji Ltd. Şti. Hyper E-Commerce Infrastructure - Storefront application and management panel allows Authentication Bypass. This issue affects Hyper E-Commerce Infrastructure: before 1.1; Hyper E-Commerce Infrastructure - dealer integration: before 1.2; Hyper E-Commerce Infrastructure - Storefront application and management panel: before 2.1796.	7.1	More Details
CVE-2026-126275	NocoDB before 2026.09.0 contains an insecure direct object reference vulnerability that allows authenticated users to read cross-base row comments by supplying only model and row ids. Attackers with a Viewer or Creator role on an unrelated base can read private comments and author emails, or plant decoy tables and duplicate comment ids to spoof teammates' comments.	7.1	More Details
CVE-2026-129153	SurveyKing 1.12.0 through 1.13.2 contains an authorization bypass in the linked survey feature that fails to verify the referenced linkSurveyId belongs to the caller's own project. Authenticated attackers can point a linked option at another user's survey so that loadLinkResult and updateLinkSurveyAnswer read, rewrite, or create responses in that survey.	7.1	More Details
CVE-2026-125830	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Belingo belingoGeo belingogeo allows Reflected XSS.This issue affects belingoGeo: from n/a through 1.13.3.	7.1	More Details
CVE-2026-124272	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 10.31.14.	7.1	More Details
CVE-2026-125837	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thethemefoundry Make make allows Reflected XSS.This issue affects Make: from n/a through 1.10.10.	7.1	More Details
CVE-2026-126463	OpenEMR before 8.5.0 contains multiple sql injection vulnerabilities that allow authenticated users to inject payloads through ERA CLP01, form_facility, form_icd_codes, and POST key names. Attackers can perform UNION, blind, and error-based injection to read users_secure password hashes and patient PHI, and overwrite patient_data fields.	7.1	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpLingua Translation Service Translate and boost SEO – Automatic AI translation – wpLingua wplingua	7.1	More

124410	allows Stored XSS.This issue affects Translate and boost SEO – Automatic AI translation – wpLingua: from n/a through 3.1.1.		Details
CVE-2026-124420	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Woody ad snippets insert-php allows Reflected XSS.This issue affects Woody ad snippets: from n/a through 2.7.10.	7.1	More Details
CVE-2026-125775	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks Forms crm-perks-forms allows Reflected XSS.This issue affects CRM Perks Forms: from n/a through 1.1.8.	7.1	More Details
CVE-2026-125764	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in E2Pdf.com e2pdf e2pdf allows Stored XSS.This issue affects e2pdf: from n/a through 1.32.65.	7.1	More Details
CVE-2026-125447	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kaliforms Kali Forms kali-forms allows Reflected XSS.This issue affects Kali Forms: from n/a through 2.4.31.	7.1	More Details
CVE-2026-125854	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unbounce Unbounce Landing Pages unbounce allows Stored XSS.This issue affects Unbounce Landing Pages: from n/a through 1.1.6.	7.1	More Details
CVE-2026-125443	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Denishua WPJAM Basic wpjam-basic allows DOM-Based XSS.This issue affects WPJAM Basic: from n/a through 7.1.2.	7.1	More Details
CVE-2026-124995	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michal Jaworski Track, Analyze & Optimize by WP Tao wp-tao allows Stored XSS.This issue affects Track, Analyze & Optimize by WP Tao: from n/a through 1.3.1.	7.1	More Details
CVE-2026-124691	In Progress Kendo UI for jQuery Gantt, the task editor's Parent dropdown renders task titles as HTML. An attacker who can influence a task title shown in the dropdown can cause attacker-controlled markup to execute as JavaScript when a user opens or interacts with the task editor. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected version is 2020.3.915; the latest vulnerable version is 2026.3.1015. The issue is fixed in version 2026.4.1111.	7.1	More Details
CVE-2026-126460	OpenEMR before 8.5.0 contains a persistent SQL injection vulnerability in SLEOB::slInvoiceNumber(), where the CLP01 claim control number from uploaded X12 835 ERA files is concatenated unescaped into a query. Attackers with billing write access can upload a crafted .edi file via sl_eob_search.php that is stored on the server and re-executes a time-based payload whenever it is reprocessed through sl_eob_process.php, extracting patient health information.	7.1	More Details
CVE-2026-125856	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sarah Giles Dynamic User Directory dynamic-user-directory allows Reflected XSS.This issue affects Dynamic User Directory: from n/a through 2.4.	7.1	More Details
CVE-2026-102589	When independent Grafana instances share the same [rendering] renderer_token, an image renderer key issued by one instance is accepted by the others, so a user on one instance could act as the user with the same ID on another (origin validation error). This affects instances with the renderAuthJWT feature toggle enabled, the default from Grafana 13.0.0.	7.1	More Details
CVE-2026-124689	In Progress Kendo UI for jQuery versions 2026.3.1014 up to, but not including, 2026.4.1110, ActionSheet does not encode title, subtitle, and header button label values before rendering them. An attacker who can influence these values can inject markup that executes as JavaScript when a user opens the ActionSheet. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The report identifies version 2026.3.1014; the first affected release has not been established.	7.1	More Details
CVE-2026-125817	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Feedzy feedzy-rss-feeds allows Stored XSS.This issue affects Feedzy: from n/a through 5.2.15.	7.1	More Details
CVE-2026-126662	Contao 4.0.0 before 5.3.54, 5.4.0 before 5.7.17, and 6.0.0 before 6.0.6 contains an access control bypass vulnerability that allows filemount-restricted backend users to modify folders outside their filemount via the file manager Edit-Multiple operation. Attackers holding the protected or syncExclude field permission can submit outside folder paths in the IDS parameter to publish protected folders or exclude them from DBAFS synchronization, exposing files for public download.	7.1	More Details
CVE-2026-124694	In Progress Kendo UI for jQuery versions 2026.3.1015 up to, but not including, 2026.4.1110, PropertyGrid does not encode bound property values and items[].description in its default configuration. An attacker who can influence either value can cause JavaScript to execute when a user views the grid. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected release has not been established.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meow Apps		More

2026-123478	AI Engine ai-engine allows Stored XSS.This issue affects AI Engine: from n/a through 3.9.1.	7.1	Details
CVE-2026-124253	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codepeople Calculated Fields Form calculated-fields-form allows DOM-Based XSS.This issue affects Calculated Fields Form: from n/a through 5.5.2.8.	7.1	More Details
CVE-2026-124693	In Progress Kendo UI for jQuery versions 2026.3.1015 up to, but not including, 2026.4.1110, PivotGrid and PivotConfigurator axis field names are passed to a chip template without appropriate encoding. An attacker who can influence an axis field name can cause JavaScript to execute when a user views the rendered chip. The field name can be interpreted as HTML in both attribute and element contexts. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected release has not been established.	7.1	More Details
CVE-2026-124692	In Progress Kendo UI for jQuery versions 2026.3.1015 up to, but not including, 2026.4.1110, the Grid and TreeList column-reorder drag clue reparses header text as HTML. An attacker who can influence a column field or title used by an affected application can cause JavaScript to execute when a user drags a column header while column reordering is enabled. Successful exploitation may compromise the confidentiality and integrity of data available in the user's browser context. The first affected release has not been established.	7.1	More Details
CVE-2026-124690	In Progress Kendo UI for jQuery, sanitizeSvgContent() parses custom icon markup into a live DOM before filtering it. An attacker who can influence custom icon content can cause JavaScript to execute during icon creation, before an unsafe element is removed. The issue was reported in version 2026.3.1015; the first affected release has not been established. The issue is fixed in version 2026.4.1110.	7.1	More Details
CVE-2026-126449	OpenEMR before 8.5.0 contains a missing authorization vulnerability in immunizations.php, diagnosis_full.php, and billing_process.php that lets low-privileged users bypass ACL checks. Authenticated Front Office users can reuse their session CSRF token to add or delete immunizations, write encounter billing codes, and invoke the billing processor.	7.1	More Details
CVE-2026-125818	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AdvancedCoding wpDiscuz wpdiscuz allows Stored XSS.This issue affects wpDiscuz: from n/a through 7.6.75.	7.1	More Details
CVE-2026-107152	An improper authentication vulnerability has been found in the task console in the smart_proxy_dynflow package. The console accepts any client certificate signed by the capsule's certificate authority. It does not check the list of servers the capsule trusts. A low-privileged network attacker or user must already hold such a certificate. They can open the console and read job details. Those details include passwords when a job was given them. They can also cancel a running task.	7.1	More Details
CVE-2026-127078	OpsTree BuildPiper before 2.7.0 contains an authorization bypass vulnerability that allows authenticated users to attach another application's environment to their service by supplying a foreign project_env_id. Attackers can configure CI and trigger builds and deployments through the component env endpoints using the other application's configuration, registries and deployment infrastructure.	7.1	More Details
CVE-2026-125760	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bit Apps Bit Assist bit-assist allows DOM-Based XSS.This issue affects Bit Assist: from n/a through 1.8.4.	7.1	More Details
CVE-2026-129429	Frappe india-payroll before 16.0.4 contains a missing authorization vulnerability in the get_employee_details, compute_tax_comparison and set_tax_regime methods of tax_regime_selector.py that allows authenticated low-privileged users to access other employees' payroll data. Attackers can supply another employee identifier to read base pay and earning and deduction components, or change the tax regime on draft Salary Structure Assignments to affect tax withholding.	7.1	More Details
CVE-2026-124688	In Progress® Kendo® UI for jQuery prior to 2026.4.1111 the TabStrip, PanelBar, and Menu widgets support mapping a dataSource field to `spriteCssClass`. If an attacker can control the mapped data, they can break out of the attribute and inject markup, including event-handler attributes. The resulting JavaScript executes in the application's origin when a victim loads a page that renders the affected widget, allowing access to data and actions available in the victim's authenticated session.	7.1	More Details
CVE-2026-67542	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.70, POST /api/mcp/fetch-tools is reachable by any authenticated user (lowest role; no admin/workflow association) and fetches an attacker-supplied URL through the sse and streamable_http transports with no scheme / private-IP / allowlist / redirect guard. The transport error is reflected in the HTTP 422 response, giving a semi-blind SSRF oracle, and the attacker also controls the outbound request headers. This issue has been patched in version 0.0.70.	7.1	More Details
CVE-2026-127077	OpsTree BuildPiper before 2.7.0 contains an authorization bypass vulnerability that allows authenticated users to create environments on unassigned Kubernetes clusters by tampering with cluster_id and namespaces values. Attackers can modify requests to POST /api/v1/project/{project_id}/env/ to target another project's cluster, then trigger builds and deployments into it, bypassing project isolation.	7.1	More Details
	In Progress® Kendo® UI for jQuery versions from 2022.2.621 prior to 2026.4.1111 the DropDownButton and		

CVE-2026-124687	SplitButton allow markup injection through the `id` and `target` attributes. An attacker who can influence these item values can break out of the attributes and inject markup, including event handlers. The issue is fixed in 2026.4.1111.	7.1	More Details
CVE-2026-116633	A potential vulnerability was reported in some Lenovo Tablets that could allow a third-party application to perform an arbitrary file write with elevated privileges.	7.1	More Details
CVE-2026-125804	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meow Apps AI Engine ai-engine allows Stored XSS.This issue affects AI Engine: from n/a through 3.9.3.	7.1	More Details
CVE-2026-128893	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marcin Wise Chat wise-chat allows Reflected XSS.This issue affects Wise Chat: from n/a through 3.4.5.	7.1	More Details
CVE-2026-111024	A user with the Viewer or Editor role could bypass folder permissions on Git Sync managed resources through the repository files API: a Viewer could read files in folders they could not access, and an Editor could create, modify, move or delete provisioned dashboards and folders there (incorrect authorization).	7.1	More Details
CVE-2026-124250	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AyeCode Ltd GeoDirectory geodirectory allows Reflected XSS.This issue affects GeoDirectory: from n/a through 2.8.202.	7.1	More Details
CVE-2026-126225	A missing authorization vulnerability in Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.7, FortiAnalyzer Cloud 8.0.0 through 8.0.1, FortiAnalyzer Cloud 7.6.7, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.7, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.7 may allow an authenticated attacker to elevate their privileges via crafted JSON-RPC request.	7.1	More Details
CVE-2026-125822	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nickboss WordPress File Upload wp-file-upload allows Stored XSS.This issue affects WordPress File Upload: from n/a through 5.2.3.	7.1	More Details
CVE-2026-111456	A missing authorization check has been found in ConsumerResource.setupOwner() function of consumer registration module in the Candlepin package. The registration method checks permission to create a consumer only when the caller is a user. A consumer that authenticates with its identity certificate does not go through that check. A low-privileged network attacker or user who has a valid consumer certificate for one organization can register a new consumer in a different organization by supplying that organization's key. The response includes an identity certificate for the new consumer. With that certificate, the attacker can view the target organization's subscription pools. When the organization is not using simple content access, the attacker can attach that organization's entitlements to the new consumer.	7.1	More Details
CVE-2026-116413	Dell PowerStore contains a use-of-broken-cryptography vulnerability. A low-privileged attacker could exploit it to impersonate another identity, potentially leading to unauthorized access.	7.1	More Details
CVE-2026-126938	Zipline before 4.6.4 contains a resource allocation vulnerability that allows authenticated users to bypass chunked-upload size and quota checks by forging Content-Range offsets and totals. Attackers can send tiny chunks to the partial upload endpoint with large declared offsets, causing the server to create oversized files and exhaust disk space.	7.1	More Details
CVE-2026-125798	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zaytech Smart Online Order for Clover clover-online-orders allows DOM-Based XSS.This issue affects Smart Online Order for Clover: from n/a through 1.6.6.	7.1	More Details
CVE-2026-126452	OpenEMR before 8.5.0 contains a missing authorization vulnerability in diagnosis_full.php that allows authenticated users to delete or clear any billing record by ID. Attackers can supply a target billing ID in the id parameter with delete or clear mode to deactivate other patients' charges and corrupt financial records.	7.1	More Details
CVE-2026-111000	A user with the Editor role who can edit a folder can move it, through the folders resource API, under a folder they administer, and so gain Admin on the moved folder and its contents, including the right to change their permissions. The legacy folder move API refuses the same move (improper privilege management).	7.1	More Details
CVE-2026-106475	The Elasticsearch data source resource proxy forwards the request method and path to Elasticsearch using the data source's own credentials, without restricting them to the operations the plugin needs. A user who can query the data source can alter index mappings or reach other indices on the cluster. [Improper authorization / path validation]	7.1	More Details
CVE-2026-95518	Time-of-check time-of-use (TOCTOU) race condition vulnerability in TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü Pardus Package Installer allows Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions. This issue affects Pardus Package Installer: from 0.7.0 before 0.7.1.	7.0	More Details
CVE-	ExcelJS through 4.4.0 contains a prototype pollution vulnerability in mergeConditionalFormattings that allows attackers to modify Object.prototype by supplying an x14:cfRule id of __proto__. Attackers can craft an xlsx file		More

2026-128337	that, when loaded with xlsx.load(), sets properties such as type, direction, border and cfvo on every object in the process until it restarts.	7.0	Details
CVE-2026-126823	A local user with an ordinary account on the same host can place a file in a shared temporary location that the JDBC driver's native library loading routine will accept and load without verifying its origin. Loading the driver class in a Java application may then run code of that user's choosing inside the application process, which may result in disclosure or alteration of data held by that process or in the process becoming unavailable.	7.0	More Details
CVE-2026-126611	Progressive Robot hMailServer 6.3.4 through 6.3.7, with a MySQL or MariaDB database, TlsMode=verify-full and no TlsCaFile, does not verify the database server's certificate's issuer or name when the connection is one that MariaDB Connector/C treats as local - Server= set to 127.0.0.1, ::1 or localhost (on Linux a Unix socket), to . on Windows (a named pipe), or to a comma-separated list of servers that holds such an element - which allows a local attacker who can stand in for the database server, for example by listening on its port while it is stopped or restarting, to receive the database sign-in, the password included, and to read and modify the traffic between hMailServer and its database. hMailServer applied verify-full by turning the client's certificate verification on without a CA file, but MariaDB Connector/C 3.4.1 and later, on a connection they treat as local and with no CA file, accept any certificate within its validity period that is self-signed or sent with its own root, for any name (Connector/C 3.4.2 to 3.4.10 also one whose issuer they cannot find), so the client accepted the certificate an impostor made, asked no proof of the password and allowed a switch to an authentication method that sends the password unhashed, while hmailserver --check-database said the certificate had been checked against the system's trust store and the application log that it had been checked. The Windows builds bundle Connector/C 3.4.9 (6.3.4 to 6.3.6) and 3.4.11 (6.3.7); on Linux the distribution's client is used, and Connector/C 3.3 and 3.4.0 and Oracle's MySQL client are not affected. The configuration is not the default: TlsMode defaults to prefer, which checks no certificate.	7.0	More Details
CVE-2026-9661	Poste Italiane Postecert FIRMAOK! 1.6.29 on Windows contains a local privilege escalation vulnerability caused by an uncontrolled OpenSSL search path, where launcher.exe and dependent executables such as updater.exe and tslupdater.exe load OpenSSL configuration and library files from a hardcoded, user-writable directory that does not exist by default. A low-privileged local attacker can create this missing directory and place malicious OpenSSL configuration or library files inside it, causing the application to load and execute attacker-controlled code with the privileges of the user running it, enabling horizontal or, when a higher-privileged user runs the application, vertical privilege escalation up to full system compromise.	7.0	More Details
CVE-2026-111521	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.4.0.17, contain a Time-of-check Time-of-use (TOCTOU) Condition vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	7.0	More Details
CVE-2026-126813	Roundcube Webmail before 1.6.21 and 1.7.x before 1.7.6 contains an IMAP command injection vulnerability that allows attackers to inject commands via CRLF in the _uid parameter when messages_cache is enabled. Attackers can lure logged-in victims into opening crafted GET links to mail/show or mail/get, executing IMAP commands that delete messages, change flags, or grant mailbox access via SETACL.	6.8	More Details
CVE-2026-81936	An internal security review identified a development regression from ThinkSystem v4 XClarity Controller 3 (XCC3) versions (2.51) IHX432Y to (2.56) IHX436K which re-introduces the default OpenBMC root password upon performing an XCC Reset to Default operation. An attacker can gain access to enabled administrative interfaces of XCC using the default OpenBMC credential re-introduced after Reset to Default. Additionally, this provides access to the underlying XCC Operating System which is not normally accessible. Only these versions are affected and are no longer available for download. Process enhancements have also been made to prevent and identify potential future regression.	6.8	More Details
CVE-2026-126431	OpenEMR before 8.5.0 contains a second-order sql injection vulnerability that allows authenticated Carecoordination users to store malicious C-CDA field identifiers through the savedata action. Attackers can inject SQL into the IN clause built by fetchFormValues() during C-CDA generation to extract password hashes, portal reset values, and patient records.	6.8	More Details
CVE-2026-119531	The Live Composer WordPress plugin before 2.1.24 does not escape several attributes of one of its page-builder shortcodes before outputting them inside HTML tag attributes, allowing users with the Contributor role and above to store a payload that executes in the browser of anyone who views the post, including an administrator reviewing the pending submission.	6.8	More Details
CVE-2026-126404	Coder 2.28.0 before 2.29.24, 2.30.0 before 2.34.16, 2.35.0 before 2.36.11, 2.37.0 before 2.37.8, and 2.38.0 before 2.38.4 does not restrict new API keys to the creating token's scopes, allow list, or expiry. A scoped API key or OAuth2 token holding key-creation permission can call POST /api/v2/users/{user}/keys/tokens to mint longer-lived coder:all keys, gaining the user's full privileges.	6.8	More Details
CVE-2026-126199	pgEdge Postgres MCP Server enables SQL queries against PostgreSQL databases through Model Context Protocol compatible clients. Prior to 1.1.0, the bundled CLI and web clients classified query_database statements only by their first keyword before deciding whether to display a write confirmation. SELECT INTO, data-modifying common table expressions beginning with WITH, and EXPLAIN ANALYZE of a write were treated as reads and could execute without confirmation on an allow_writes connection. Read-only connections remain protected by PostgreSQL transaction access mode, and EXPLAIN without ANALYZE and SELECT FOR UPDATE remain classified as reads. This issue is fixed in 1.1.0.	6.8	More Details

CVE-2026-126855	Missing authorization in ImageCapture in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	6.8	More Details
CVE-2026-92738	Vault's Login MFA feature did not consistently enforce the lifetime of pending two-phase login requests. This may allow a user who previously completed the first authentication factor to complete MFA and obtain a Vault token after the pending request should have expired, including after the user's primary credential has been rotated. This vulnerability (CVE-2026-92738) is fixed in Vault Community Edition 2.2.2 and Vault Enterprise 2.2.2, 1.21.14, and 1.19.26.	6.8	More Details
CVE-2026-127091	Jadaptive Maverick Synergy Server before 3.0.33 and 3.1.x before 3.1.7, and Maverick Legacy Server before 1.8.1, contain an improper path equivalence flaw in VirtualFileFactory.canonicalisePath that bypasses mount-level access policy. Authenticated users can supply paths with duplicate separators or dot segments to route operations to a less restrictive parent mount and read or write files the child mount denies.	6.8	More Details
CVE-2026-129118	C-Kermit 8.0.200 before 11.1.515 contains an improper certificate hostname validation vulnerability that allows attackers to impersonate hosts by abusing wildcard matching in dNSName_cmp() in ck_ssl.c. Attackers holding a trusted certificate with over-matching names containing asterisks, question marks, brackets, or empty labels can intercept credentials and data over Telnet, FTP, and HTTP TLS connections.	6.8	More Details
CVE-2026-117522	The Dynific Addons for Elementor (formerly Anywhere Elementor) WordPress plugin before 1.3.1 does not escape the post title before outputting it in a quoted HTML attribute in one of its Elementor widgets, allowing authenticated users with the Author role to publish a post whose title executes as script in the session of anyone, including an administrator, who views it, resulting in Stored Cross-Site Scripting.	6.8	More Details
CVE-2026-126295	NLTK from 3.10.0 before 3.10.4 contains an arbitrary file read vulnerability in BllipParser that allows attackers to open files outside NLTK data roots by supplying unvalidated model paths. Attackers controlling parser_model, reranker_features, reranker_weights, or from_unified_model_dir() input can make the bllipparser C extension read sensitive files or block on FIFOs and devices.	6.8	More Details
CVE-2026-111033	The Countdown, Coming Soon, Maintenance WordPress plugin through 3.0.8 does not perform authorization or nonce checks when saving countdown data on post save, and its output-sanitization allowlist permits script tags, allowing users with Author-level access and above to store arbitrary web scripts that execute when the affected content is viewed on the front end or in an administrator session.	6.8	More Details
CVE-2026-118421	The WP Directory Kit WordPress plugin before 1.6.3 does not properly sanitise and escape a parameter used to order results on one of its admin screens before using it in a SQL statement, relying on a keyword deny-list whose replacement order can be bypassed, making it possible for users holding the WP Directory Kit WordPress plugin before 1.6.3's custom Listing Admin role, and above, to perform SQL injection attacks.	6.8	More Details
CVE-2026-110072	The Photo Gallery by 10Web WordPress plugin before 1.8.49 does not escape a shortcode attribute that sets a gallery watermark image before rendering it into an HTML image attribute, and decodes percent-encoded characters in the value, allowing users with Contributor-level access and above to perform Stored Cross-Site Scripting that executes in the browser of any user, including an administrator, who views the published gallery.	6.8	More Details
CVE-2026-129117	C-Kermit 8.0.200 before 11.1.515 contains an improper certificate validation vulnerability that allows machine-in-the-middle attackers to impersonate Telnet servers because ssl_reply() never calls ssl_check_server_name(). Attackers can refuse START-TLS, offer Telnet AUTHENTICATION SSL, and present any trusted CA certificate to capture user credentials and session data.	6.8	More Details
CVE-2026-126941	Zipline through 4.6.2 contains an authorization bypass vulnerability that allows authenticated administrators to read superadmin secrets because GET /api/users and GET /api/users/:id lack the canInteract check. Attackers can retrieve plaintext totpSecret and OAuth tokens to bypass 2FA and take over superadmin accounts, while any authenticated user can enumerate other users' folders via GET /api/user/folders.	6.8	More Details
CVE-2026-104718	The Elementor Website Builder WordPress plugin before 4.3.6 does not validate or escape an element identifier before rendering it into a client-side framework attribute that is evaluated as JavaScript, allowing users with the Contributor role to store scripts that execute in the browser of anyone viewing the affected content, including an administrator reviewing the submission for publication.	6.8	More Details
CVE-2026-75489	Cudy TR3000 before 2.5.42 contains an insufficient verification of data authenticity vulnerability in the mt_wifi Smart Mesh Technology (SMT) onboarding, which protects messages only with an AES-CBC key derived from public values and a CRC32 check. Adjacent unauthenticated attackers can forge SMT messages in Probe Request vendor IEs carrying an attacker-chosen SSID and pre-shared key, forcing unpaired devices to join attacker-controlled access points.	6.8	More Details
CVE-2026-86343	An improper neutralization of CRLF sequences vulnerability in the SNMP API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users with administrator privileges to read or write arbitrary files and conduct denial-of-service attacks.	6.8	More Details
CVE-2026-	Use of hard-coded credentials (CWE-798) on the 1300 communications board in DJI AeroScope Mobile (TP703) firmware 03.00.00.26, with 1300 communications board firmware 02.00.07.12 through 02.00.08.40, allows an attacker with physical access to the board's serial console to log in as root. The same password hash is present on every unit and uses DES crypt, so the password can be recovered offline from the distributed firmware. No	6.8	More

128910	network login service accepts this password by default. Confirmed on a physical device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. DJI has discontinued AeroScope Mobile and no fixed firmware is available.		Details
CVE-2026-118420	The WP Directory Kit WordPress plugin before 1.6.3 does not sanitise and escape a parameter before using it in a SQL statement, making it possible for users holding the WP Directory Kit WordPress plugin before 1.6.3's custom Listing Admin role, and above, to perform SQL injection attacks.	6.8	More Details
CVE-2026-117521	The Dynific Addons for Elementor (formerly Anywhere Elementor) WordPress plugin before 1.3.1 does not escape a user-controlled profile value before outputting it in a quoted attribute in one of its Elementor widgets, allowing authenticated users with the Author role to store a payload that executes in the session of anyone, including an administrator, who views a post the attacker authored, resulting in Stored Cross-Site Scripting.	6.8	More Details
CVE-2025-59847	HCL Domino Leap is vulnerable to Stored XSS through malicious application titles in Manage page dialogs, allowing an attacker to take over a user's session	6.8	More Details
CVE-2025-59848	HCL Leap is vulnerable to Stored XSS through malicious application titles in the Manage page dialogs, allowing an attacker to take over a user's session	6.8	More Details
CVE-2026-121527	A execution with unnecessary privileges vulnerability in Fortinet FortiClientEMS 7.4.3 through 7.4.7, FortiClientEMS 7.4.0 through 7.4.1, FortiClientEMS 7.2 all versions may allow an authenticated local attacker with admin privileges to gain root shell access via CLI commands.	6.7	More Details
CVE-2026-126625	Incorrect default permissions in the Windows installer of Progressive Robot hMailServer 6.3.7 allow a local authenticated user to run code as the administrator who installs the product, when it is installed into a new program folder in a location whose permissions let every user write, such as the root of a drive. 6.3.7 fixed CVE-2026-107571 by giving the program folder, Bin and ControlPanel permissions that only administrators may change, but its setup lets Inno Setup make a new program folder first, with the permissions the folder above hands down, and replaces them only afterwards, tens of milliseconds later (33 to 139 milliseconds in the project's test runs). In that time any local account may make files and folders in the new folder, which keep that account as their owner, among them the Bin folder that setup then copies the programs into. Setup runs programs from Bin with the administrator's elevated rights, registering the service among them, before its hardening at the end of setup takes such a folder back, and those programs load a library placed in Bin in place of the system's. The default installation under Program Files, whose folders give ordinary users read and execute only, is not affected.	6.7	More Details
CVE-2025-71463	Scapy before 2.7.0 contains an insecure deserialization vulnerability in the load_session function that allows attackers to execute code by supplying a malicious pickle session file. Attackers can trick users into loading a crafted .pkl.gz file via the -s option or conf.session, executing embedded Python code through __reduce__().	6.7	More Details
CVE-2026-129260	A security vulnerability has been detected in Mereithhh VanBlog up to 0.54.0. This vulnerability affects the function fs.readFileSync of the file local.provider.ts of the component Custom Page Handler. The manipulation of the argument path leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version test-20261013 is able to resolve this issue. The identifier of the patch is d63aa163f10b6dc1080e2368fe8e71aa95b765cb. Upgrading the affected component is advised.	6.6	More Details
CVE-2026-116468	A flaw was found in the group-move and organization group reparenting endpoints of the keycloak-services component. This component is responsible for core authentication and authorization services in the Red Hat build of Keycloak. The issue occurs because the system fails to check if a target parent group confers administrative roles when a group is moved. A delegated administrator can exploit this to move a group they control under an administrative group, causing all members to inherit full realm-admin privileges and gain complete control over the realm.	6.6	More Details
CVE-2026-68862	Dell Terraform Provider for Dell PowerFlex contain(s) an OS Command Injection Vulnerability in the SDC host provisioning component. A high privileged remote attacker with access to the PowerFlex management plane could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on provisioned SDC hosts. Exploitation may lead to full compromise of affected SDC hosts.	6.6	More Details
CVE-2026-123790	ComfyUI-Easy-Use version 1.3.6 contains a path traversal vulnerability in the `save_preview()` handler for POST `/easyuse/save/{name}`. The handler checks the source directory before appending a user-supplied filename and allows the request to select the `custom_nodes` directory as a copy destination. An unauthenticated attacker who can reach the ComfyUI server can overwrite an installed custom node’s Python entry point with an uploaded file. When ComfyUI restarts and loads the modified node, the attacker’s code runs with the privileges of the ComfyUI process.	6.5	More Details
CVE-2026-129119	C-Kermit from 6.0.192 before 11.1.515 contains a file collision protection bypass that allows malicious senders to append data to existing files by marking transfers as RESEND. The gattr() function in ckcfn3.c clears the REJECT discard flag and switches to APPEND without a RECEIVE CONFIRM prompt, letting attackers modify files such as shell startup files.	6.5	More Details
	NocoDB before 2026.06.2 contains an attachment size limit bypass that allows authenticated Editor users to		

CVE-2026-126293	store oversized files because data-attachment-v3.service.ts trusts the remote server's advertised content length. Attackers can point the v3 upload-by-URL endpoint at a server that understates or omits its length to exhaust disk space or storage quota.	6.5	More Details
CVE-2026-126453	OpenEMR before 8.5.0 contains an inverted comparison in Document::has_expired() that causes the FHIR Binary download endpoint to treat time-limited PHI documents as unexpired after their one-hour lifetime. Authenticated users still authorized for a Binary/{id} resource can download expired bulk export NDJSON files and $docref CCDs indefinitely.	6.5	More Details
CVE-2026-126835	The MongoDB Node.js driver does not consistently enforce its permitted-host restriction during OIDC authentication. A bearer token produced by the embedding application's own login callback may therefore be transmitted to a host outside the configured set of permitted hosts, which may result in unintended disclosure of that credential. No database account is required; the party supplying the connection configuration needs only to influence the settings the application passes to the driver.	6.5	More Details
CVE-2026-129160	free-fs 2.0.1 through 2.3.1 contains an SQL injection vulnerability in FileShareServiceImpl.getPages, which passes the orderBy parameter of the /apis/share/pages endpoint verbatim into the ORDER BY clause via MyBatis-Flex without a column whitelist. Authenticated users can supply CASE WHEN subquery expressions that use share ordering as a boolean oracle to read arbitrary database contents, such as share codes.	6.5	More Details
CVE-2026-124041	Catalis/Patriot Properties WebPro 5.0 allows a remote unauthenticated attacker to execute arbitrary SQL queries against the underlying MSSQL database, enabling exfiltration of sensitive property and taxpayer information.	6.5	More Details
CVE-2026-58265	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, a BACnet/SC peer can trigger a heap out-of-bounds read (up to 3 bytes), pre-authentication, in the BACnet/SC header-option decoder. bvlc_sc_decode_proprietary_option() reads the vendor-id and option-type at fixed offsets [3],[4],[5] before checking the option's declared header length, and the option-list validator never enforces a minimum length for proprietary options. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	6.5	More Details
CVE-2026-129121	C-Kermit 8.0.200 before 11.1.515 contains a path traversal vulnerability in doftpget() in ckcftp.c that allows malicious FTP servers to write files outside the intended directory. Attackers can return absolute paths, tilde names, or dot-dot components in NLST or MLSD listings during MGET /RECURSIVE to overwrite files like .bashrc, leading to code execution.	6.5	More Details
CVE-2026-126403	Coder 2.26.0 before 2.29.24, 2.30.0 before 2.34.16, 2.35.0 before 2.36.11, 2.37.0 before 2.37.8, and 2.38.0 before 2.38.4 contains an improper authorization flaw in the external agent credentials endpoint, which returns the workspace agent token to users with only workspace read access rather than ssh permission. Authenticated users with roles such as Template Admin or Organization Admin can use the token to read the owner's private Git SSH key and Git provider OAuth tokens, and impersonate the agent to receive the owner's sessions.	6.5	More Details
CVE-2026-129129	AiSOC 12.1.0 before 23.3.0 contains a missing authentication vulnerability that allows unauthenticated attackers to query the enrichment service through Next.js console rewrite routes. Attackers can send requests to /api/v1/enrichment/lookup or /api/v1/enrichment/bulk to retrieve threat-intelligence results and set force to true to consume commercial provider API quota.	6.5	More Details
CVE-2026-129166	Keep 0.34.10 through 0.55.0 contains a blind SQL injection vulnerability in its CEL-to-SQL converter, which inserts bracket-indexed JSON keys from CEL filters unescaped into JSON path expressions for SQLite, PostgreSQL, and MySQL. Authenticated users with read:alert permission can submit crafted CEL expressions to /alerts/query or the cel parameter of /incidents, using result counts as a boolean oracle to extract other tenants' alerts and password hashes.	6.5	More Details
CVE-2026-126429	OpenEMR before 8.5.0 passes authenticated user-controlled HTML from the doc_lib.php content parameter to mPDF, which resolves local files and nested SVG resources. Authenticated patients or core users can submit crafted CSS imports or php://filter SVG references to read arbitrary server files including credentials and OAuth keys.	6.5	More Details
CVE-2026-129130	agent-device from 0.21.36 before 0.21.37 contains a local file disclosure vulnerability that allows authenticated remote callers to read daemon-host files by opening file:// URLs. Attackers can send an open command with a file:// target through /rpc, then issue snapshot to read any plaintext file readable by the daemon account.	6.5	More Details
CVE-2026-126399	vLLM from 0.19.0 before 0.31.0 contains a resource exhaustion vulnerability that allows inference clients to bypass the server frame limit by setting media_io_kwargs.video.num_frames in chat completion requests. Attackers can supply num_frames=-1 or a large value with many base64 JPEG frames, forcing VideoMediaIO to decode all frames and np.stack them, causing memory exhaustion.	6.5	More Details
CVE-2026-127211	MultiVendorX plugin for WordPress before 5.0.22 contains a broken access control vulnerability in the /wp-json/multivendorx/v1/stores REST route that allows authenticated vendors to access administrative flag handlers due to the store_owner role possessing the edit_stores capability and missing per-store ownership checks. Attackers can exploit the insecure direct object reference in the visitorMap handler and other flag handlers to retrieve other stores' contact emails, pending withdrawal amounts, onboarding and registration data, deactivation reasons, and visitor analytics, resulting in a cross-tenant confidentiality breach.	6.5	More Details

CVE-2026-127121	SOGo before 5.12.13 contains an improper cryptographic signature verification vulnerability that allows remote attackers to replace a victim's contact S/MIME certificate by sending a spoofed multipart/signed message with a mismatched signature and an impersonated From address. Attackers can deliver a crafted CMS signedData object containing their own self-signed certificate, which SOGo's UIxMailView stores on the contact card without validating signature authenticity or certificate identity, enabling subsequent encrypted communications to be decrypted with the attacker's private key.	6.5	More Details
CVE-2026-126290	NocoDB before 2026.07.0 contains an information disclosure vulnerability in base-integrations.service.ts that allows authenticated base members to read private integration configurations by omitting a query flag. Attackers can request another user's private integration without the configuration flag, bypassing the ownership check to obtain stored connection credentials.	6.5	More Details
CVE-2026-116509	The Quiz and Survey Master (QSM) – Quiz Maker & Survey Maker plugin for WordPress is vulnerable to generic SQL Injection via the 'qpages' parameter in all versions up to, and including, 11.2.9 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 contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The injected payload survives storage and a published-status check in display_shortcode() because a non-numeric ID causes the isPublished lookup to return an empty string, after which the payload is imploded directly into a WHERE question_id IN() clause via plain string interpolation with no wpdb->prepare() or esc_sql() call.	6.5	More Details
CVE-2026-63164	Omnispace Agora Project through 26.10.0 contains an insecure direct object reference vulnerability that allows authenticated attackers to access another user's private mail by supplying a crafted reloadMailTypeId parameter to Ctrl::getCurObj() without a readRight() ownership check in CtrlMail.php. Attackers can manipulate the mail identifier value, such as reloadMailTypeId=mail-1, to retrieve the title and body of private messages belonging to other users, resulting in unauthorized disclosure of sensitive communications.	6.5	More Details
CVE-2026-126267	NocoDB from 0.300.0 before 2026.04.4 contains a denial of service vulnerability that allows authenticated users to crash the server by triggering an unhandled promise rejection in MetaService metadata logging. Attackers can send a request leaving a lookup condition undefined, causing knex binding errors in the unawaited logHelper call that terminate the server process.	6.5	More Details
CVE-2026-89037	Dolibarr before 24.0.2 contains an insecure direct object reference vulnerability in the REST Documents API for the ticket module that allows authenticated API users to access ticket attachments belonging to other companies by omitting a company-scope check that is only applied via a session variable set during public ticket authentication, which REST API authentication never sets. Attackers with ticket read permission can enumerate predictable ticket identifiers and supply them to the documents endpoint or download path to retrieve sensitive attachments such as invoices and contracts belonging to other third parties.	6.5	More Details
CVE-2026-126461	OpenEMR before 8.5.0 contains a missing authorization vulnerability in library/ajax/user_settings.php that lets any authenticated user persist arbitrary global configuration overrides. Attackers can POST global:-prefixed keys to re-point external service hosts like CouchDB, eRx, phiMail, or SMTP to attacker-controlled servers, exfiltrating system credentials and patient PHI.	6.5	More Details
CVE-2026-127216	Injection Guard plugin for WordPress before 1.4.0 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to trigger password hash export by tricking a logged-in administrator into loading a crafted link, since the ig_settings admin page in templates/dashboard.php processes GET parameters without nonce verification. Attackers can exploit this to cause the plugin to write WooCommerce customer email hashes and password hashes to an unprotected file at wp-content/plugins/injection-guard/ab-hash.dat, which can then be downloaded without authentication to obtain customer password hashes for offline cracking.	6.5	More Details
CVE-2026-126270	NocoDB before 2026.09.1 contains a missing authentication vulnerability in the aggregated meta info route of utils.controller.ts that exposes instance-wide metadata to anonymous callers. Unauthenticated attackers can request the endpoint to enumerate bases, user counts, shared and password-protected view counts, webhook counts, and live per-base row counts, while repeated requests amplify database query load.	6.5	More Details
CVE-2026-122227	The Easy Property Listings plugin for WordPress is vulnerable to generic SQL Injection via the 'post_type' parameter in all versions up to, and including, 3.5.28 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The sanitize_text_field() function is applied to the attribute value but does not escape single quotes, providing no mitigation against breaking out of the SQL IN('...') literal.	6.5	More Details
CVE-2026-126272	NocoDB before 2026.09.0 contains an uncontrolled resource consumption vulnerability that allows authenticated users to bypass bulk row-count limits by using session authentication instead of API tokens. Attackers with Editor write permission on one table can submit hundreds of thousands of rows to v1 and v2 bulk write routes, exhausting database connections, CPU, and memory.	6.5	More Details
CVE-2026-	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.4 and 1.5.1, there is a client-side out-of-bounds read in the AtomicReadFile-ACK record-access handling path. The issue is caused by a mismatch between a remote returnedRecordCount value and the fixed local fileData[] array capacity in BACNET_ATOMIC_READ_FILE_DATA. The ACK decode path preserves the remote RecordCount,	6.5	More

46677	discards storage for excess records without truncating that count, and a downstream sink later iterates over the original RecordCount and indexes fileData[i] out of bounds. This issue has been patched in versions 1.4.4 and 1.5.1.		Details
CVE-2026-126457	OpenEMR before 8.5.0 contains a missing authorization vulnerability in InstallerController that allows any authenticated user to modify module administration settings without the admin/manage_modules permission. Low-privileged users such as Front Office clerks can POST to saveConfig, DeleteAcl, DeleteHooks and nickName actions to reconfigure or partially disable installed modules.	6.5	More Details
CVE-2026-122063	The Newsletters plugin for WordPress is vulnerable to blind SQL Injection via the 'user_email' parameter in all versions up to, and including, 4.18.2 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 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. Exploitation requires the admin-controlled 'currentusersubscribed' option to be enabled and at least one page rendering the Newsletters subscribe shortcode or widget to exist; a Subscriber-level attacker can self-serve the attack by updating their own profile email to a crafted payload and loading such a page.	6.5	More Details
CVE-2026-93335	Vault Community Edition and Vault Enterprise did not consistently apply explicit ACL policy deny rules to request paths that differ only by a trailing slash. This may allow an authenticated user who holds a broader delete permission on system configuration paths to disable a secrets engine, auth method, or audit device that a more specific deny rule was intended to protect. This vulnerability (CVE-2026-93335) is fixed in Vault Community Edition 2.2.2 and Vault Enterprise 2.2.2, 1.21.14, and 1.19.25.	6.5	More Details
CVE-2026-126443	OpenEMR before 8.5.0 contains a missing authorization vulnerability in dynamic_finder_ajax.php that allows authenticated users without patients/demo permission to query patient demographics. Attackers can supply arbitrary patient_data columns via the sColumns parameter to enumerate names, dates of birth, contact details, and Social Security numbers across the practice.	6.5	More Details
CVE-2026-126465	OpenEMR before 8.5.0 contains an SQL injection vulnerability in the patient portal api/onsiteactivityviews endpoint that allows any authenticated staff user to inject SQL through unquoted Id_BitwiseAnd Criteria values. Attackers can close the bitwise parenthesis and append OR or UNION SELECT clauses to read patient PHI, staff password hashes, MySQL authentication strings, and API tokens.	6.5	More Details
CVE-2026-126405	Coder 2.21.0 before 2.29.24, 2.30.0 before 2.34.16, 2.35.0 before 2.36.11, 2.37.0 before 2.37.8, and 2.38.0 before 2.38.4 reads Web Push endpoint responses in webpushSend with io.ReadAll, without a size limit or client timeout. Any authenticated user can register a subscription via POST /api/v2/users/{user}/webpush/subscription pointing to a server returning an endless body, exhausting coderd memory and crashing the API, dashboard, and workspace connections.	6.5	More Details
CVE-2026-127141	SOGo before 5.12.13 contains a denial of service vulnerability that allows authenticated attackers to exhaust all worker processes by configuring an auxiliary IMAP mail account pointing to a controlled host that accepts a TCP connection but never sends an IMAP greeting response. Attackers can issue concurrent GET requests to the mail view of this account to hold workers indefinitely without an effective timeout, occupying every SOGo worker and denying service to all users for approximately five minutes until the watchdog kills and respawns the stuck workers.	6.5	More Details
CVE-2026-126415	OpenEMR before 8.5.0 contains a missing authorization vulnerability in the Patient Validation module that allows any authenticated user to retrieve patient demographic records. Attackers can send direct requests with wildcard mf_lname or empty mf_ parameters to the patientvalidation endpoint to enumerate the entire patient_data table.	6.5	More Details
CVE-2026-128100	Vault Community Edition and Vault Enterprise did not apply explicit ACL policy deny rules to letter case variants of user and group names in auth methods that treat these names as case-insensitive. This may allow an authenticated user with delegated permissions to modify a protected user or group, potentially leading to privilege escalation. This vulnerability (CVE-2026-128100) is fixed in Vault Community Edition 2.2.2 and Vault Enterprise 2.2.2, 1.21.14, and 1.19.25.	6.5	More Details
CVE-2026-126281	NocoDB before 2026.08.0 contains a missing authorization vulnerability in the copy-from branch of integration creation in integrations.service.ts that decrypts a source integration's connection credentials without checking its owner or private flag. Authenticated users with the Creator role can supply guessed or enumerated integration ids to copy other users' private database host, username, and password into an integration they own.	6.5	More Details
CVE-2026-128077	Nuxt is an open-source web development framework for Vue.js. From 4.6.0 until 4.6.4, Nuxt parses a request path beginning with // as a URL host before rendering a page, while Nitro server/middleware and routeRules continue to evaluate the original path. An unauthenticated request such as //x/admin can therefore resolve to the /admin page without route-scoped serverHandlers, server/middleware path checks, redirects, or security headers configured for /admin. API handlers in server/api and server/routes, appMiddleware, page middleware are unaffected. This issue is fixed in version 4.6.4.	6.5	More Details
CVE-	Grafana is an open-source platform for monitoring and observability. When an Elasticsearch data source is configured with a time-based index pattern, Grafana generated one index name for every interval in the requested query time range without any upper limit. A user with permission to query the data source, which		More

2026-81843	includes users holding only the Viewer role in a default configuration, could submit a single small query with an extreme time range and cause the server to allocate memory until it was terminated. The allocation occurred before any request was sent to Elasticsearch, so the condition applied whether or not the Elasticsearch cluster was reachable. Data sources configured with a static index name are not affected.	6.5	Details
CVE-2026-126437	OpenEMR before 8.5.0 contains an authorization bypass vulnerability in portal/lib/download_template.php that allows any authenticated core user to render documents for arbitrary patients by setting isModule. Attackers can submit arbitrary pid and template_id values to disclose patient names, birth dates, chart IDs, addresses, allergies, medications, and problem lists despite ACL and squad restrictions.	6.5	More Details
CVE-2026-126467	OpenEMR before 8.5.0 contains a mass assignment vulnerability in ObservationController::processEnhancedFormSave() that allows authenticated low-privilege users to forge authorization flags through an incomplete field blacklist. Attackers can submit authorized=1 or override the id field alongside observation_id to mark observations as Provider-signed and overwrite clinical fields of other observations within the same patient encounter.	6.5	More Details
CVE-2026-129104	Cudy TR3000 before 2.5.42 contains a dnsmasq configuration injection vulnerability that allows authenticated administrators to inject directives by embedding a newline in the net.set_dhcp leasetime field. Attackers can append address= entries via /etc/init.d/dnsmasq to alter DNS answers for LAN clients, or insert invalid lines that stop dnsmasq.	6.5	More Details
CVE-2026-128071	Nuxt is an open-source web development framework for Vue.js. Nuxt from 3.0.0 until 4.6.4, @nuxt/nitro-server from 3.20.0 until 4.6.4, and @nuxt/vite-server from 4.6.0 until 4.6.4, routeRules matching leaves an encoded slash (%2F) in the request path while a catch-all page such as app/pages/[...slug].vue or a custom multi-segment page route decodes it into a route parameter. The getRouteRules result is therefore incomplete, and an unauthenticated request can render the page without the redirect, headers, proxy, SSR, noScripts, appMiddleware, or appLayout rules configured for the decoded path. Protected content is resolved only when the page interprets the decoded parameter accordingly: a custom multi-segment parameter can contain the decoded path, while a repeatable catch-all must join the slash-containing array element; route.path remains encoded and does not resolve that resource. Static pages, single-segment parameters, server/api handlers, and server/routes handlers are not affected because they do not have the same encoded-path mismatch. This issue is fixed in version 4.6.4.	6.5	More Details
CVE-2026-110189	IBM ContextForge MCP Gateway 1.0.8 through 1.0.11, and v1.1.0 is vulnerable to denial of service due to an incomplete denylist in the jq filter guard module (CWE-184). An authenticated remote attacker can supply a crafted `jsonpath_filter` value containing `halt`, `halt_error`, or unbounded-loop built-ins that bypass the safety check, causing gateway worker process termination or sustained resource exhaustion.	6.5	More Details
CVE-2026-127213	LearnPress Course Wishlist Add-on before 4.1.2 contains an insecure direct object reference vulnerability that allows remote attackers to manipulate any user's course wishlist by supplying an arbitrary user_id parameter to the render_button callback instead of relying on the session identity. Attackers can exploit the publicly accessible load_content_via_ajax REST route, which only requires a public wp_rest nonce, to add or remove courses from any user's wishlist and determine whether a given course is wishlisted by iterating user_id and course_id values.	6.5	More Details
CVE-2026-129105	Cudy TR3000 before 2.5.42 contains an option injection vulnerability that allows authenticated administrators to inject arbitrary pppd options by embedding quotes and newlines in L2TP credentials. Attackers can submit crafted usernames or passwords to the net.set_wan RPC method, which l2tp.sh writes into a pppd options file, adding options like logfile to the root pppd process.	6.5	More Details
CVE-2026-63167	Omnispace Agora Project through 26.10.0 contains a SQL injection vulnerability that allows authenticated general administrators to inject arbitrary SQL by setting the personsSort session value, which is concatenated unsanitized into ORDER BY clauses in MdlUser.php and MdlSpace.php. Attackers can submit an error-based extractvalue payload through personsSort to leak database information, such as the MariaDB version, via the user and space listing pages.	6.5	More Details
CVE-2026-126319	Dockhand before 1.0.55 contains an arbitrary file read vulnerability that allows authenticated users with stacks:create permission to read sensitive files by supplying an arbitrary composePath during stack adoption. Attackers can adopt a stack pointing to the encryption key, SQLite database, or /proc/self/environ and read it via the compose endpoint to obtain all stored credentials.	6.5	More Details
CVE-2026-129432	Ettercap through 0.8.5.1 contains a heap out-of-bounds read vulnerability in dissector_mountd() in src/dissectors/ec_mountd.c that validates RPC credential and directory lengths independently rather than against the packet end. Network-adjacent attackers can send a crafted MOUNT MNT call to read up to 100 bytes past the heap buffer, leaking memory to the console and logs.	6.5	More Details
CVE-2026-77706	Improper handling of highly compressed data (data amplification) vulnerability in Fileorbis Bilişim Hizmetleri Ticaret Anonim Şirketi FileOrbis NextGen FileServer allows Sustained Client Engagement. This issue affects FileOrbis NextGen FileServer: before 12.7.	6.5	More Details
CVE-2026-125708	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 10.0.4.	6.5	More Details

CVE-2026-126332	Improper access control in the autofill vault search in Devolutions Server 2026.3.13.0 and earlier allows an authenticated user with only view permission on a shared entry to obtain its password in clear text via a linked credential entry created in their private vault.	6.5	More Details
CVE-2026-125454	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Passster content-protector allows Stored XSS.This issue affects Passster: from n/a through 4.3.21.	6.5	More Details
CVE-2026-125450	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force SureRank surerank allows Stored XSS.This issue affects SureRank: from n/a through 1.10.3.	6.5	More Details
CVE-2026-125433	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FuturioWP Futurio Extra futurio-extra allows Stored XSS.This issue affects Futurio Extra: from n/a through 2.0.25.	6.5	More Details
CVE-2026-123702	The Security For WooCommerce WordPress plugin through 1.0.16 does not check that the requester is authorised before regenerating the secret keys and salts in the site's configuration file, allowing unauthenticated users to log out every user and, on servers that cannot reach the WordPress.org API, corrupt the configuration file and take the whole site offline.	6.5	More Details
CVE-2026-125045	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in John-Michael L'Allier Create mediavine-create allows Stored XSS.This issue affects Create: from n/a through 3.1.1.	6.5	More Details
CVE-2026-126327	Improper access control in the connection history in Devolutions Server 2026.3.13.0 allows an authenticated user without the permission to view passwords to obtain historical entry passwords via the connection history API.	6.5	More Details
CVE-2026-126326	Improper access control in the administrative role assignment endpoint in Devolutions Server 2026.3.13.0 and earlier allows an authenticated user with only vault assignment management rights to escalate privileges and read vault entry passwords via a crafted role assignment request.	6.5	More Details
CVE-2026-127076	OpsTree BuildPiper before 2.7.0 contains a broken access control vulnerability that allows authenticated users to list and build from Git repositories restricted to other projects. Attackers can enumerate repositories via GET /api/v1/git_repo/?all=true and submit any git_repo_id to the ci endpoint, cloning other projects' source code, manifests, and committed secrets.	6.5	More Details
CVE-2026-127075	OpsTree BuildPiper before 2.7.0 contains a path traversal vulnerability that allows authenticated users to read arbitrary files by supplying traversal sequences in Additional Manifest file paths. Attackers can enter paths like ../../../../etc/passwd so the renderer embeds file contents in generated manifests and logs, exposing configuration files and service-account tokens.	6.5	More Details
CVE-2026-105440	Missing authorization in the JSON-RPC web services interface of Extreme Networks Switch Engine (EXOS) allows an authenticated, low-privileged (read-only) user to execute CLI show commands that are restricted to that role through the command line interface. Successful exploitation results in disclosure of sensitive information, including the device configuration and the password hashes of local accounts. Configuration, enable, and debug commands are not affected. Disclosed password hashes can be attacked offline, and a weak password could lead to administrative access to the device. This issue is fixed in Switch Engine 33.7.1-patch1-11, 33.1.100.133-patch1-9, and 32.7.4.15-patch1-11. Extreme Networks would like to thank Toàn Lê (GitHub: https://github.com/toanln-cov) for responsibly disclosing this vulnerability and for working with our PSIRT team through coordinated disclosure.	6.5	More Details
CVE-2026-124418	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ahmad WP Job Portal wp-job-portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.7.2.	6.5	More Details
CVE-2026-124495	When workers run as the topology owner, the Logviewer serves files that a worker has placed in its own log directory as links to other files. A user who is allowed to submit topologies can read the worker logs of other users' topologies, and other files the Logviewer process can read. Users are recommended to upgrade to version 3.2.0, which fixes the issue.	6.5	More Details
CVE-2026-125781	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NOUS Ouvert Utile et Simple Event post event-post allows Stored XSS.This issue affects Event post: from n/a through 6.1.2.	6.5	More Details
CVE-2026-15198	A missing authentication for critical functionality vulnerability in the Webdav API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers to read specific files and conduct limited denial-of-service attacks.	6.5	More Details
CVE-2026-125816	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PT Norther Lights Production MapSVG mapsvg-lite-interactive-vector-maps allows Stored XSS.This issue affects MapSVG: from n/a through 9.0.4.	6.5	More Details
CVE-			

2026-124411	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force SureCart surecart allows Stored XSS.This issue affects SureCart: from n/a through 4.12.1.	6.5	More Details
CVE-2026-124752	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 10.0.3.	6.5	More Details
CVE-2026-123473	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 3.51.0.	6.5	More Details
CVE-2026-107509	A user with the Viewer role can make Grafana allocate an unbounded amount of memory, and crash it, with a single SQL Expression query that casts a value to a very large BINARY length (memory allocation with excessive size value).	6.5	More Details
CVE-2026-14242	A user with the Editor role could delete, move, push or pull Git Sync managed resources in folders where they only had view access, by creating a provisioning job through the jobs resource API, which skipped the folder permission checks (incorrect authorization).	6.5	More Details
CVE-2026-125743	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements addon-elements-for-elementor-page-builder allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.5.	6.5	More Details
CVE-2026-121776	Missing Authorization vulnerability in WP Chill Passster content-protector allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Passster: from n/a through 4.3.20.	6.5	More Details
CVE-2026-128025	FrankenPHP before 1.13.0 contains a path-split interpretation conflict in splitPos in cgi.go that allows unauthenticated attackers to execute protected PHP scripts by embedding .php inside a filename component. Attackers can request paths like /uploads/a.php.txt/b.php to execute uploads/a.php despite route-level or WAF deny rules and forge PATH_INFO, SCRIPT_NAME, and PHP_SELF values.	6.5	More Details
CVE-2026-126818	A Ruby object-document mapper does not apply its automatic field-level encryption configuration to certain fields when the data model uses class inheritance. Values the application designated for encryption are written to the database in readable form without any error or warning. A database account holding only read access to the application's collections, and no access to the encryption key store, may obtain those values.	6.5	More Details
CVE-2026-128016	FrankenPHP before 1.13.4 contains a use-after-free vulnerability in worker mode that frees internal streams of SplTempFileObject or SplFileObject on php://temp instances surviving across requests. Remote clients can send requests reaching code that uses such persisted objects, causing reads of freed memory that leak garbage data or crash the process.	6.5	More Details
CVE-2026-128015	FrankenPHP before 1.13.4 contains a use-after-free vulnerability that leaves a dangling pointer to a freed environment table when putenv() is called during request shutdown. Attackers triggering putenv() in shutdown functions, destructors, or session handlers can crash the process on the next getenv() call or leak previous request environment values.	6.5	More Details
CVE-2026-125831	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IdeaBox Creations PowerPack Lite for Beaver Builder powerpack-addon-for-beaver-builder allows Stored XSS.This issue affects PowerPack Lite for Beaver Builder: from n/a through 1.3.2.	6.5	More Details
CVE-2026-119102	In Telerik UI for Blazor, versions v12.0.0 through 15.2.0, an improper input validation vulnerability exists, where the Grid, TreeList and Gantt's AI command filters on any model property, bypassing the declared column allowlist.	6.5	More Details
CVE-2026-125833	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YITH YITH WooCommerce Ajax Product Filter yith-woocommerce-ajax-navigation allows Stored XSS.This issue affects YITH WooCommerce Ajax Product Filter: from n/a through 5.24.0.	6.5	More Details
CVE-2026-126320	Dockhand before 1.0.55 contains an improper authorization vulnerability that lets users holding only containers:view download arbitrary container files instead of requiring containers:exec. Authenticated Enterprise RBAC users can request any path from the files/download endpoint, which reads through Docker's archive API, to retrieve secrets, keys, and mounted credentials.	6.5	More Details
CVE-2026-94125	Nimbus returns the worker placement of every topology running on a supervisor, including the host, port, owner and resource assignment of topologies the caller is not authorized to read. In a multi-tenant cluster, an authenticated user who is allowed to access Nimbus can learn where the workers of other users' topologies run. Users are recommended to upgrade to version 3.2.0, which fixes the issue.	6.5	More Details
CVE-2026-125762	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LeapWorx Premium Addons for Elementor premium-addons-for-elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.11.116.	6.5	More Details
	A user who can create Git Sync provisioning jobs (the Editor role by default) could delete or move files outside		

CVE-2026-110992	the configured repository path with a job that references a resource whose source path contains ../ sequences (path traversal). With a local filesystem repository on versions before 13.0.4 and 13.1.1, this reached files on the Grafana host.	6.5	More Details
CVE-2026-123006	The repository search used by the dashboard (`GET /repo/search`) returned the internal commit status object of each repository. Since 28.0.0 that object included the repository owner's full user record, so any signed-in user could read the password hash, salt and email address of the owner of any repository they can see that has a commit status. The response now contains only the state and target URL of the commit status.	6.5	More Details
CVE-2026-13721	A user with edit access to one folder could modify, move or delete Git Sync provisioned resources in folders where they only had view access, through the provisioning files API (incorrect authorization).	6.5	More Details
CVE-2026-129355	A vulnerability has been found in sigoden dufs up to 0.46.0. This affects an unknown part of the file src/server.rs of the component WebDAV COPY Operation Handler. The manipulation leads to incorrect authorization. The attack is possible to be carried out remotely. Upgrading to version 0.47.0 is able to mitigate this issue. The identifier of the patch is fba13dffb9c65b5e5e26419f64de709200277a04. It is advisable to upgrade the affected component.	6.5	More Details
CVE-2026-129454	Zr.Admin.NET commit 85cff6a through commit eb9228a contains an insecure direct object reference vulnerability in GET /workflow/instance/{instanceId} that lets logged-in users view others' workflow instances. Authenticated low-privilege attackers can enumerate sequential instance IDs to read other users' approval requests, including submitted form contents, applicant details and approval records.	6.5	More Details
CVE-2026-126934	Zipline 4.3.2 before 4.8.0 contains a rate limit bypass vulnerability that allows unauthenticated attackers to evade throttling by spoofing X-Forwarded-For headers when core.trustProxy is enabled. Attackers can send a different X-Forwarded-For value per request to obtain fresh rate-limit buckets, enabling unlimited guessing of login passwords, TOTP codes, and file and URL passwords.	6.5	More Details
CVE-2026-124755	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Kruit Advanced Custom Fields: Font Awesome Field advanced-custom-fields-font-awesome allows Stored XSS.This issue affects Advanced Custom Fields: Font Awesome Field: from n/a through 6.1.4.	6.5	More Details
CVE-2026-129431	Ettercap through 0.8.5.1 contains a heap out-of-bounds read vulnerability in dissector_socks() in src/dissectors/ec_socks.c that allows network-adjacent attackers to read heap memory via unchecked SOCKS5 username/password lengths. Attackers can send a crafted SOCKS5 authentication packet observed by Ettercap to read up to 255 bytes past the heap buffer, disclosing memory printed and logged as captured credentials.	6.5	More Details
CVE-2026-128037	In gittuf 0.10.0 through 0.15.0, when a minimum threshold global rule and a policy rule protect the same namespace, verification gives the global rule's check over all trusted users in the policy precedence over the policy rule's own authorized users. A user listed in the policy file but not authorized by the policy rule, or fewer users than the rule's threshold, can make changes to the protected namespace that pass verification.	6.5	More Details
CVE-2026-125785	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine jet-engine allows Stored XSS.This issue affects JetEngine: from n/a through 3.9.1.	6.5	More Details
CVE-2026-67540	Heym builds and runs agentic systems and business-process automations on self-hosted infrastructure. Prior to version 0.0.70, get_workflow_template / get_node_template fetches a template by ID with no visibility / author / shared_with predicate, so any authenticated user can read (and use) any other tenant's private (visibility=specific_users) template — including its full node/edge graph and the email addresses it was shared with. The list endpoint enforces visibility correctly; the single-item get/use paths do not. This issue has been patched in version 0.0.70.	6.5	More Details
CVE-2026-120991	When a container blob upload was rejected, for example because it exceeded a package size quota, the cleanup removed the blob from storage even if the same content already existed and was used by other packages. On an instance with a package quota configured, a user who can upload container images and has the exact content of another owner's package file or image layer could make it undownloadable. The cleanup now only removes blobs that the failed upload created.	6.5	More Details
CVE-2026-16550	An external control of file name or path vulnerability in the Media Parser in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write arbitrary files.	6.5	More Details
CVE-2026-124965	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rtCamp Inc. rtMedia for WordPress, BuddyPress and bbPress buddypress-media allows Stored XSS.This issue affects rtMedia for WordPress, BuddyPress and bbPress: from n/a through 4.7.16.	6.5	More Details
CVE-2026-126483	OpenEMR before 8.5.0 contains an SQL injection vulnerability that allows authenticated report users to manipulate queries by supplying a crafted form_facility value to interface/reports/ippf_statistics.php. Attackers can close the string literal in the facility_id WHERE clause and use boolean or time-based payloads to read sensitive database contents.	6.5	More Details

CVE-2026-122671	Missing Authorization vulnerability in E2Pdf.com e2pdf e2pdf allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects e2pdf: from n/a through 1.32.65.	6.5	More Details
CVE-2026-126641	A host key verification flaw was found in ansible-pylibssh and in the ansible.netcommon libssh connection plugin. When trust-on-first-use is enabled (host_key_auto_add on the libssh connection plugin, or AutoAddPolicy in ansible-pylibssh), a host that is already present in known_hosts but now presents a different key is accepted without warning. The pylibssh Session.verify_knownhost() method passes the SSH_KNOWN_HOSTS_CHANGED and SSH_KNOWN_HOSTS_OTHER states to the same missing_host_key() policy hook used for unknown hosts, and the bundled AutoAddPolicy/RejectPolicy classes (as well as ansible.netcommon's MyAddPolicy, which is modeled on paramiko's AutoAddPolicy) therefore add the changed key and continue the connection rather than aborting as paramiko's BadHostKeyException path would. As a result the controller authenticates to the substitute host, runs the play there, and appends the new key to known_hosts, which can disclose connection credentials to an attacker performing a machine-in-the-middle attack. Default configurations (host_key_checking enabled, host_key_auto_add unset) are not affected; non-interactive runs fail closed.	6.5	More Details
CVE-2026-125800	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Stored XSS.This issue affects Spectra: from n/a through 2.20.5.	6.5	More Details
CVE-2026-126643	A cleartext storage flaw was found in the AAP Gateway Operator. When reconciling an AutomationController, the operator reads the protected resource-server Secret (Secret/<aap-name>-resource-server, key controller_resource_server_secret) and copies its plaintext value into the generated AutomationController custom resource under spec.extra_settings (RESOURCE_SERVER.SECRET_KEY). Although the operator uses no_log to keep the value out of its own logs, serializing it into the custom resource exposes it to any principal able to read the AutomationController CR without permission to read the backing Kubernetes Secret, breaking the expected OpenShift RBAC separation between the two resources. The value may also propagate into Kubernetes API/etcd storage, GitOps and Argo diffs and history, rendered manifests, support bundles, and audit data. The resource-server secret is intended for trusted Gateway-to-Controller service authentication, and its disclosure may allow a user to impersonate a trusted Controller service and reach privileged service-index APIs.	6.5	More Details
CVE-2026-117373	Janus WebRTC Server 1.2.3 through 1.4.0 is vulnerable to Directory Traversal. The application accepts a caller supplied media path when an ondemand stream is created. The path is validated only by checking whether it contains one of the audio extensions and is then passed to the file source which opens it. No canonicalization is performed and no directory allowlist is enforced, so an unauthenticated caller can make the server open an arbitrary local file and use it as a media source, with the content delivered to viewers as RTP audio.	6.5	More Details
CVE-2026-125807	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HTMega HT Mega ht-mega-for-elementor allows Stored XSS.This issue affects HT Mega: from n/a through 3.2.8.	6.5	More Details
CVE-2026-116559	The A2Reviews WordPress plugin through 1.2.3 does not properly verify authorization on several of its API command handlers, relying on a signature keyed on a value that is empty by default on an unconnected install, allowing unauthenticated attackers to modify A2Reviews WordPress plugin through 1.2.3 settings and product review metadata and to read non-public product metadata.	6.5	More Details
CVE-2026-116333	Buffer over-read in PostgreSQL parallel B-tree scans allows an object creator to read attacker-chosen server-memory addresses, via a function incorrectly marked PARALLEL SAFE or STABLE to make participating workers build different scan-key arrays. Within major versions 17-18, minor versions before PostgreSQL 18.7 and 17.12 are affected. Versions before PostgreSQL 17 are unaffected.	6.5	More Details
CVE-2026-124256	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeRockz Delivery & Pickup Date Time for WooCommerce woo-delivery allows Stored XSS.This issue affects Delivery & Pickup Date Time for WooCommerce: from n/a through 1.3.90.	6.5	More Details
CVE-2026-118975	In Progress® Telerik® Reporting prior to version 20.3.26.1110, improper restriction of XML external entity references in the SVG processing engine allows an authenticated attacker with low privileges who can supply SVG content to a report to read local or UNC files, or trigger server-side network requests, from the report rendering host. External XML entities in SVG content were resolved without applying the configured strict resource resolver and report path validation. Disclosed content is limited by the permissions of the rendering process and by what the rendered report output exposes.	6.5	More Details
CVE-2026-121773	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GeneratePress GenerateBlocks generateblocks allows Stored XSS.This issue affects GenerateBlocks: from n/a through 2.5.0.	6.5	More Details
CVE-2026-125857	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sarah Giles Dynamic User Directory dynamic-user-directory allows Stored XSS.This issue affects Dynamic User Directory: from n/a through 2.4.	6.5	More Details
CVE-2026-124257	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wordplus BP Better Messages bp-better-messages allows Stored XSS.This issue affects BP Better Messages: from n/a through 3.2.1.	6.5	More Details

CVE-2026-125809	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in myCred myCred mycred allows Stored XSS.This issue affects myCred: from n/a through 4.0.2.	6.5	More Details
CVE-2026-119518	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WProyal Royal Elementor Addons royal-elementor-addons allows Stored XSS.This issue affects Royal Elementor Addons: from n/a through 1.7.1070.	6.5	More Details
CVE-2026-125824	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Go Maps WP Go Maps wp-google-maps allows Stored XSS.This issue affects WP Go Maps: from n/a through 10.1.10.	6.5	More Details
CVE-2026-125805	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AyeCode Ltd GeoDirectory geodirectory allows Stored XSS.This issue affects GeoDirectory: from n/a through 2.8.204.	6.5	More Details
CVE-2026-126471	OpenEMR before 8.5.0 contains a missing authorization vulnerability in print_referral.php and trend_form.php that allows low-privileged Front Office users to access patient PHI without patients:med permission. Attackers can directly request these endpoints with arbitrary patient_id values to retrieve patient demographics, insurance data, and vitals history, enumerating IDs to expand disclosure.	6.5	More Details
CVE-2026-125801	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Automattic WooCommerce woocommerce allows Leveraging Race Conditions.This issue affects WooCommerce: from 11.0.0 through 11.2.2.	6.5	More Details
CVE-2026-125761	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YITH YITH WooCommerce Ajax Search yith-woocommerce-ajax-search allows Stored XSS.This issue affects YITH WooCommerce Ajax Search: from n/a through 2.30.0.	6.5	More Details
CVE-2026-125796	Missing Authorization vulnerability in Ahmad JS Help Desk js-support-ticket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JS Help Desk: from n/a through 5.0.5.	6.5	More Details
CVE-2026-126940	Zipline before 4.6.4 contains a rate limit bypass vulnerability that allows remote attackers to evade request limits by varying query strings or supplying the x-zipline-p-filename header. Attackers can append differing query parameters to login and file or short-link password verification endpoints to perform credential guessing beyond the intended rate limits.	6.5	More Details
CVE-2026-125835	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetTabs jet-tabs allows Stored XSS.This issue affects JetTabs: from n/a through 2.3.5.	6.5	More Details
CVE-2026-119302	The NotificationX WordPress plugin before 3.3.7 does not perform any capability, authentication or nonce check on its notification preview path, allowing unauthenticated users to disclose the content of private, draft, pending and password-protected posts and to execute arbitrary registered shortcodes by supplying crafted preview data on any front-end request.	6.5	More Details
CVE-2026-87801	An insertion of sensitive information into sent data vulnerability in the API framework in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read arbitrary files.	6.5	More Details
CVE-2026-123480	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fullworks Plugins Display Eventbrite Events widget-for-eventbrite-api allows Stored XSS.This issue affects Display Eventbrite Events: from n/a through 6.9.1.	6.5	More Details
CVE-2026-126817	A flaw in the automatic client-side encryption schema generation of the Mongoid ODM may cause values that an application declared for encryption to be written and stored as cleartext when more than one model is mapped onto the same storage location. No error or warning is raised. A party holding an ordinary read-only database account, with no access to the encryption key material, may then obtain those values in clear form.	6.5	More Details
CVE-2026-121721	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PublishPress Gutenberg Blocks advanced-gutenberg allows Stored XSS.This issue affects Gutenberg Blocks: from n/a through 3.7.6.	6.5	More Details
CVE-2026-125451	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Blocks b-blocks allows Stored XSS.This issue affects B Blocks: from n/a through 2.1.15.	6.5	More Details
CVE-2025-41725	Affected devices running firmware versions prior to 4.1.0 may crash and become unavailable when receiving specific malformed Bluetooth messages from an unauthenticated attacker.	6.5	More Details
CVE-2026-91868	IBM Security QRadar EDR 3.12 through 3.12.26 could allow a remote authenticated attacker to obtain sensitive information due to improper access control.	6.5	More Details

CVE-2026-61417	Dell SmartFabric OS10 Software, versions prior to 10.6.0.10, contains an Improper Access Control vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	6.5	More Details
CVE-2026-125794	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hupe13 Extension for Leaflet Map extensions-leaflet-map allows Stored XSS.This issue affects Extension for Leaflet Map: from n/a through 6.1.1.	6.5	More Details
CVE-2026-126642	An incorrect authorization flaw was found in AWX, the automation controller component of Red Hat Ansible Automation Platform. The API access classes for JobTemplate and WorkflowJobTemplate do not check the caller's Credential use_role when assigning the single-valued webhook_credential foreign key: JobTemplateAccess.can_add/can_change and WorkflowJobTemplateAccess.can_change in awx/main/access.py omit the check_related('webhook_credential', Credential, ..., role_field='use_role') call that UnifiedCredentialsMixin.can_attach performs for the normal many-to-many credentials relationship, and the serializer validates only the credential's type and namespace. A user who may administer their own job template (or workflow job template) and use its project and inventory can therefore attach a webhook token credential (for example a GitLab token) that they do not have use permission on. The template administrator can retrieve the template's webhook key; a subsequent webhook event causes AWX to decrypt the attached token and send it in the request header (for GitLab, PRIVATE-TOKEN) to a status URL derived from the event payload, disclosing the victim's token to a destination the attacker can influence. This may disclose another user's personal access token and allow whatever actions that token permits.	6.5	More Details
CVE-2026-125455	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bold Themes Bold Page Builder bold-page-builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 5.9.11.	6.5	More Details
CVE-2026-124653	The Mine CloudVod WordPress plugin before 2.6.6 does not restrict who can request cloud storage upload credentials from several of its REST API routes, allowing unauthenticated attackers to obtain signed upload policies and temporary credentials for the site's configured Alibaba Cloud OSS, Tencent Cloud COS and Dogecloud accounts and use them to upload or overwrite files in the site's storage.	6.5	More Details
CVE-2026-125680	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bold Themes Bold Page Builder bold-page-builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 5.9.11.	6.5	More Details
CVE-2026-105983	The Email Marketing 4Dem WordPress plugin through 2.0.5 does not perform authorization or capability checks on several of its AJAX actions and REST routes, allowing unauthenticated users to disclose the Email Marketing 4Dem WordPress plugin through 2.0.5's stored configuration and data and to modify its stored settings.	6.5	More Details
CVE-2026-125853	Missing Authorization vulnerability in Everestthemes Everest Backup everest-backup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Everest Backup: from n/a through 2.3.15.	6.5	More Details
CVE-2026-94407	IBM ContextForge MCP Gateway 1.0.0 through 1.0.11 is potentially vulnerable to denial of service due to uncontrolled regular expression complexity (CWE-400 / ReDoS). An authenticated user with tool-registration privileges can embed catastrophically backtracking regex patterns in a tool's JSON Schema `pattern` field; when ContextForge validates arguments against that schema, the validation call may consume unbounded CPU, potentially degrading gateway availability.	6.5	More Details
CVE-2026-126410	Wasmtime's wasmtime-wasi crate 48.0.0 before 48.0.8, 49.0.0 before 49.0.5, and 50.0.0 before 50.0.1 contains a time-of-check/time-of-use race in the wasip3 wasi:sockets udp-socket host implementation that lets guests bypass socket_addr_check send restrictions. A malicious guest can race udp-socket.send against udp-socket.connect to deliver attacker-controlled datagrams to addresses the policy permits only for receiving.	6.4	More Details
CVE-2026-120658	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'file[additional_previews][]' parameter in all versions up to, and including, 7.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The wpdm_sanitize_array() function strips HTML tags via wp_kses but leaves bare single quotes intact and calls stripslashes_deep() which defeats WordPress magic quotes protection, allowing a single-quote-based attribute breakout payload to be stored verbatim and later rendered without escaping.	6.4	More Details
CVE-2026-65973	Laradocs maintains version-controlled documentation inside a Laravel codebase. From version 0.4.0 to before version 1.0.0, Laradocs is vulnerable to local command injection in server-side KaTeX rendering via an unescaped Node.js binary path in a proc_open() command string. This issue has been patched in version 1.0.0.	6.4	More Details
CVE-2026-126029	The WPZOOM Addons for Elementor – Starter Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'actions[save_builder][data][elements][...][settings][regions][i][link][url] / [pins][i][link][url]' parameter in all versions up to, and including, 1.4.20 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
	The Recipe Card Blocks Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'steps[].text'		

CVE-2026-125948	parameter in all versions up to, and including, 3.7.0 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. Because wp_kses_post() preserves block-delimiter HTML comments verbatim on save, a Contributor can embed event-handler payloads inside the block's steps[].text attribute in a draft or pending post without the unfiltered_html capability, and the payload executes for any visitor — including privileged editors and administrators who preview or publish the post — as well as through the public print endpoint.	6.4	More Details
CVE-2026-119097	The Author Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' parameter in all versions up to, and including, 4.9.3 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-2026-128026	FrankenPHP from 1.5.0 before 1.13.0 contains an incomplete environment sandbox vulnerability in which putenv writes to the process-wide OS environment via os.Setenv, leaking values across concurrent requests. Attackers reaching a request path that spawns child processes with the default environment through proc_open or exec can read secrets such as database passwords set by other requests.	6.4	More Details
CVE-2026-123667	The Photo Engine (Media Organizer & Lightroom) WordPress plugin before 6.6.2 does not sanitise and escape keyword names before storing them and outputting them on its debugging page, allowing users with the Author role and above to perform Stored Cross-Site Scripting attacks against administrators who have enabled that page.	6.4	More Details
CVE-2026-120573	The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_category' parameter in all versions up to, and including, 2.9.1 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. The injected payload is persisted in post meta as campaign_data, bypassing wp_kses sanitization, and executes in the browser session of any user with edit_posts — including Administrators — who opens the WPeMatico campaigns list screen.	6.4	More Details
CVE-2026-125409	The Passster – Password Protect Pages and Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'metavalue (metakeyinput=passster_id | passster_headline)' parameter in all versions up to, and including, 4.3.21 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. A Contributor can break out of the shortcode attribute context by embedding a] character in the passster_id or passster_headline meta value to prematurely close the opening shortcode tag, then append a [/passster] closing tag so that the trailing HTML payload is emitted verbatim by do_shortcode() — bypassing the per-attribute escaping present inside render_shortcode() — and the script will also execute in an editor's or administrator's browser when they preview the Contributor's pending post, since filter_the_content() has no edit-permission capability gate.	6.4	More Details
CVE-2026-116419	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, containsan Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	6.4	More Details
CVE-2026-127217	Post to Google My Business plugin for WordPress before 3.5.7 contains a blind server-side request forgery vulnerability that allows authenticated users with Contributor-level privileges or higher to make the server send requests to arbitrary hosts by supplying an unvalidated mbp_post_attachment URL that reaches a raw getimagesize() call in validate_external_image_size() via the preview REST route. Attackers can exploit this to perform internal port scanning, probe internal-only services and cloud metadata endpoints, and trigger GET-based side effects on internal systems, bypassing network perimeter controls since the request originates from the web server.	6.4	More Details
CVE-2026-116421	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	6.4	More Details
CVE-2026-119035	The Schema & Structured Data for WP & AMP WordPress plugin before 1.70 does not safely encode its structured data output when the Pretty Print option is enabled, allowing users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks when the site maps a schema property to a custom field.	6.4	More Details
CVE-2026-82102	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery vulnerability.	6.4	More Details
CVE-2026-110531	The FV Player 8 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fv_player_videos' parameter in all versions up to, and including, 8.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the administrator-controlled "Allow visitors to upload videos to their profile" setting to be enabled, without which the vulnerable save routine is inaccessible to Subscriber-level users.	6.4	More Details
CVE-	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, containsan Insertion of Sensitive Information into Log		

2026-116420	File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	6.4	More Details
CVE-2026-127050	Backup Migration before 2.1.8 for WordPress contains a path traversal vulnerability in its PclZip restore fallback that allows an attacker to achieve arbitrary file write when an administrator restores a malicious backup archive on a server lacking the PHP zip extension. Attackers can craft a zip archive with entry names containing ".." sequences, which PclZip's extract() processes without the PCLZIP_OPT_EXTRACT_DIR_RESTRICTION option, writing a PHP file outside the intended extraction directory into the web-servable tree to achieve remote code execution.	6.4	More Details
CVE-2026-18742	The Flatsome theme for WordPress is vulnerable to Stored Cross-Site Scripting via 'data-text-sec', 'data-title', and 'title' Attributes via Custom HTML Block in all versions up to, and including, 3.20.12 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 survives server-side sanitization because wp_kses_post permits data-* attributes globally via _wp_add_global_attributes, allowing attacker-controlled values in data-text-sec, data-title, and title attributes to persist in saved post content and be later interpreted as HTML by the ux-countdown, scroll-to, and lightbox-gallery JavaScript behaviors.	6.4	More Details
CVE-2026-127083	Huginn from 2026.09.09 before 2026.11.09 contains a server-side request forgery vulnerability because OutboundProxy.configure! applies the egress proxy only to Faraday and Typhoeus. Authenticated users can configure JiraAgent or WeiboPublishAgent to send HTTParty, open-uri or Net::HTTP requests directly to internal services, with JiraAgent returning response data as events.	6.4	More Details
CVE-2026-129357	A vulnerability was determined in Linux Foundation Magma up to 1.9.0. This issue affects the function hostOrgMiddleware of the file nms/server/host/middleware.ts of the component Host Middleware. This manipulation of the argument role causes missing authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-126279	NocoDB before 2026.06.2 contains a stored cross-site scripting vulnerability in PromptWithFields.vue that renders unescaped field references from AI field prompts as HTML in a tooltip. Attackers with the Creator role or above can store markup in a prompt's field reference that executes when victims open the field configuration, stealing the localStorage session token to call authenticated APIs as the victim.	6.3	More Details
CVE-2026-106472	Grafana's Prometheus data source passes the resource path supplied by the caller to the configured Prometheus server without restricting it to the supported API endpoints [missing path allowlist]. A user with permission to query the data source can read responses from other endpoints on that server using the data source's credentials.	6.3	More Details
CVE-2026-106133	In Progress® Telerik® Report Server prior to version 12.3.26.1110, an incorrect authorization vulnerability in the Web Report Designer allows an authenticated attacker with low privileges to perform unauthorized operations on shared report resources, affecting their integrity and availability.	6.3	More Details
CVE-2026-129443	A vulnerability was determined in itsourcecode Airline Reservation System 1.0. The impacted element is an unknown function of the file /admin/manage_user.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-126994	A vulnerability has been found in braindecode up to 1.8.1. Affected is the function resolve_type_kwargs of the file braindecode/models/util.py of the component Model Config Deserialization. Such manipulation of the argument Activation leads to use of externally-controlled input to select classes or code. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.0.0 is able to address this issue. The name of the patch is 05b764d93b9a50400f523206fbe03d73d0cf5edb. The affected component should be upgraded.	6.3	More Details
CVE-2026-125858	Missing Authorization vulnerability in CleverReach CleverReach® WP cleverreach-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CleverReach® WP: from n/a through 1.5.26.	6.3	More Details
CVE-2026-126276	NocoDB before 2026.08.1 contains an authentication bypass vulnerability in oauth-token.service.ts that treats PKCE as a substitute for confidential client authentication, skipping client secret verification when omitted. Attackers holding a captured authorization code and PKCE verifier can mint access tokens and 60-day refresh tokens for a confidential client without knowing its secret.	6.3	More Details
CVE-2026-126995	A vulnerability was found in tjake Jlama up to 0.8.4/0.9.0-beta. Affected by this vulnerability is the function SafeTensorIndex.loadWeights of the file jlama-core/src/main/java/com/github/tjake/jlama/safetensors/SafeTensorIndex.java. Performing a manipulation of the argument weight_map results in path traversal. The attack may be initiated 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-	REVA is an interoperability platform. Prior to versions 2.40.5 and 2.46.4, Reva exposes internal metadata folders		More

2026-57500	in the spaces of an authenticated user. This can lead to unwanted ways of interaction with the data. This issue has been patched in versions 2.40.5 and 2.46.4.	6.3	Details
CVE-2026-126418	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability in interface/billing/sl_eob_invoice.php, which escapes billing codes for HTML attributes but not for JavaScript strings in an inline onkeyup handler. Clinicians with encounter coding access can save crafted billing codes through diagnosis.php that execute script when a Back Office user enters a payment, exposing patient and financial data or performing actions as that user.	6.3	More Details
CVE-2026-116422	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and Information exposure.	6.3	More Details
CVE-2026-126381	n8n before 2.43.5, 2.44.x before 2.44.1, and 3.x before 3.0.1 contains an SQL injection vulnerability in the Vector Store (OracleDB) node, which does not validate Metadata Filter keys used in vector search queries. Attackers can supply crafted filter keys through untrusted workflow input such as webhooks to read data accessible to the configured Oracle credential.	6.3	More Details
CVE-2026-126996	A vulnerability was determined in SakanaAI text-to-LoRA 0.0.1. Affected by this issue is the function get_tokenizer of the file src/hyper_llm_modulator/utils/model_loading.py of the component Checkpoint Loading. Executing a manipulation of the argument base_model_name_or_path can lead to path traversal. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-124745	A flaw was found in BusyBox. When extracting an archive, the tar utility improperly resolves deferred hardlink targets across symbolic links pointing outside the intended extraction directory. An attacker could provide a specially crafted archive that links to sensitive files outside the extraction tree, allowing subsequent extraction operations to overwrite arbitrary files on the system.	6.3	More Details
CVE-2026-127086	Ryot before 10.5.6 contains an authorization bypass vulnerability that allows authenticated users to take over other users' collections by supplying an updateId to the createOrUpdateCollection GraphQL mutation. Attackers who know a collection id can trigger ownership reassignment without checks, read its items, rewrite metadata, and evict the original owner and collaborators.	6.3	More Details
CVE-2026-124744	A flaw was found in BusyBox. When extracting files using the cpio utility with path traversal protection enabled, hardlink target paths are not properly sanitized. By tricking a user or automated process into extracting a crafted archive, an attacker can create hardlinks that point to files outside the intended extraction directory. This issue may allow an attacker to modify or overwrite arbitrary files outside the target directory during subsequent extraction operations.	6.3	More Details
CVE-2026-128886	A flaw was found in dbus when configured with the nonce-tcp transport. An unauthenticated attacker able to connect to an exposed listener can cause a Denial of Service (DoS) by opening a connection and withholding the expected authentication token. Because the server processes this verification without enforcing a timeout, the stalled connection blocks the accept process and prevents legitimate clients from establishing new connections.	6.2	More Details
CVE-2026-128987	A flaw was found in dbus. A local attacker can exploit this vulnerability by connecting to an affected service, requesting a response, and stopping socket reads while keeping the connection open. Because the socket transport handles broken pipe write errors as retryable, the application enters a continuous retry loop. This can lead to excessive CPU consumption, resulting in a denial of service (DoS) for the target process.	6.2	More Details
CVE-2026-129478	Assimp through 6.0.6 contains a heap out-of-bounds read vulnerability in glTFCommon::Util::ParseDataURI caused by storing the data offset in a signed char. Attackers can supply a crafted glTF file with a raw data URI whose segment starts beyond byte 127 to crash applications or leak adjacent heap memory.	6.1	More Details
CVE-2026-129154	SurveyKing 1.13.0 through 1.13.2 contains a stored cross-site scripting vulnerability because the server accepts a respondent-supplied survey snapshot and the frontend renders its titles via innerHTML. Anonymous respondents can submit a forged snapshot embedding event handlers such as img onerror that execute in an administrator's browser session when the response is viewed.	6.1	More Details
CVE-2025-71465	@kolkov/angular-editor before 3.0.3 contains a cross-site scripting vulnerability in refreshView() that writes HTML from ngModel or reactive form controls to innerHTML without DomSanitizer, bypassing the default sanitize option. Attackers can store HTML with event-handler attributes in content later loaded into the editor to execute script in the application's origin for users opening it.	6.1	More Details
CVE-2026-126203	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. From 2.21.0 until 2.25.3, Loofah's HTML5 APIs Loofah.html5_fragment, Loofah.html5_document, and the scrub_html5_* methods can emit sanitized output that a browser reparses as different markup when used with Nokogiri before 1.19.5, because those Nokogiri versions do not escape angle brackets in attribute values. MathML can place markup inside an allowed attribute so the reparsed output becomes live HTML. The :strip scrubber is affected in every browser, while :prune and :escape are affected in WebKit browsers. Loofah's HTML4 APIs, Loofah::Helpers.sanitize, :whitewash, rails-html-sanitizer's default configuration, and JRuby are not affected. This issue is fixed in version 2.25.3.	6.1	More Details
CVE-	FileCodeBox 2.2.1 through 2.8.4 contains a stored cross-site scripting vulnerability in renderMarkdownPreview,		

2026-129170	which returns unsanitized text when the marked parser throws. Unauthenticated attackers can share text with thousands of nested blockquote markers followed by HTML payloads, executing script that steals the admin token from localStorage.	6.1	More Details
CVE-2026-63166	Omnispace Agora Project through 26.10.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious HTML markup by controlling imported directory data or an uploaded CSV file, as values are rendered into table cell text and value attributes after only Txt::utf8Encode() with no HTML escaping in VuePersonsImportExport.php. Attackers can craft a CSV cell containing an attribute-breakout payload that is rendered verbatim and executed in the browser of the administrator performing the import, leading to arbitrary script execution in the administrative context.	6.1	More Details
CVE-2026-127235	A reflected cross-site scripting vulnerability exists in the web user interface of multiple versions of OpenNMS Meridian and Horizon. Several web UI pages copy request parameter values into the HTML response without correct contextual output encoding. A remote attacker can craft a link that runs arbitrary JavaScript in the OpenNMS origin when an authenticated user opens it. The script runs in the victim's browser with the victim's session, so the attacker can read page data and send same-origin requests as the victim. The fix encodes the affected request values. On pages that use AngularJS, the fix also stops client-side template evaluation of the reflected values. The solution is to upgrade to Meridian 2024.3.15, 2025.0.12, 2026.0.2 and Horizon 36.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	6.1	More Details
CVE-2026-126476	OpenEMR before 8.5.0 contains a reflected cross-site scripting vulnerability in the Application module's auto-suggest endpoint, which echoes the searchMode POST parameter unencoded into a single-quoted onClick attribute. Attackers can induce an authenticated user to submit a single-quote payload to application/index/search, executing arbitrary JavaScript in that user's session to steal session cookies or disclose patient data.	6.1	More Details
CVE-2026-129447	Kroki before 0.36.0 contains a reflected cross-site scripting vulnerability in the /dbml/svg endpoint that allows unauthenticated attackers to inject javascript: hyperlinks by supplying crafted DBML table url, headercolor, or TableGroup color settings. Attackers can send a crafted SVG link that, when opened and the table header clicked, executes attacker JavaScript in the Kroki origin.	6.1	More Details
CVE-2026-126475	OpenEMR before 8.5.0 contains a reflected cross-site scripting vulnerability that allows authenticated attackers to execute JavaScript by injecting payloads into the searchEleNo POST parameter of the application/index/search endpoint. Attackers can break out of unencoded HTML attributes in auto-suggest.phtml to inject event handlers that fire on DOM insertion, stealing non-HttpOnly session cookies and patient data.	6.1	More Details
CVE-2026-126474	OpenEMR before 8.5.0 contains a reflected cross-site scripting vulnerability in the ACL module that allows attackers to execute JavaScript in authenticated sessions via the module_id parameter. Attackers can deliver crafted acl/index or acl/acl links that inject unencoded input into inline script blocks, stealing non-HttpOnly session cookies and modifying ACL configuration.	6.1	More Details
CVE-2026-127092	BuildAdmin 1.0.1 through 2.3.9 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to store javascript: URLs in the admin operation log via the X-Rewrite-URL header. When an administrator clicks the log entry's url open button, the script runs in the backend origin and steals the adminInfo token from localStorage, enabling account takeover.	6.1	More Details
CVE-2026-126563	Semantic MediaWiki 2.4.0 before 7.4.1 contains a reflected cross-site scripting vulnerability in TimeValueFormatter::getCaptionFromFreeFormat(), which emits free-format date captions in HTML without escaping. Unauthenticated attackers can craft a Special:Ask URL with HTML markup in a date printout format (#-F[...]) to execute script in a logged-in victim's browser session.	6.1	More Details
CVE-2025-71464	@kolkov/angular-editor before 3.0.4 contains a cross-site scripting vulnerability in toggleEditorMode() that assigns source view text to innerHTML without DomSanitizer sanitization. Attackers can induce users to paste HTML with event handlers such as img onerror into source mode, executing script in the application's origin when toggling views.	6.1	More Details
CVE-2026-129168	PMail 2.9.1 through 2.9.8 contains a stored cross-site scripting vulnerability because the /attachments/{id}/{cid} endpoint returns email attachments verbatim with the sender-supplied Content-Type after cid: references are rewritten into attachment links. Unauthenticated SMTP senders can email a text/html attachment and a page-covering cid link, so a recipient who clicks the message runs script in their webmail session to change passwords, including the administrator's.	6.1	More Details
CVE-2026-128040	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a stored cross-site scripting vulnerability because admin pages render Dataflow profile link variables, tax rate titles, OAuth consumer names, and PayPal certificate filenames without escaping. An administrator restricted to one affected area can store script that runs when another administrator, including a full administrator, opens the page, reading the form key and performing actions with that administrator's privileges.	6.1	More Details
CVE-2026-63155	Omnispace Agora Project through 26.10.0 contains an open redirect vulnerability that allows remote attackers to redirect users to arbitrary external URLs by manipulating the objUrl parameter in Ctrl.php's redir() function. Attackers can craft login links with objUrl set to a malicious site, causing the application to issue an HTTP 302 redirect to that external URL, which can be abused for phishing and credential theft.	6.1	More Details

CVE-2025-71462	Zipline before 3.7.12 contains a cross-site scripting vulnerability in the login page that allows attackers to execute JavaScript by supplying an unvalidated url parameter. Attackers can craft a login link with a javascript: URI in the url parameter that executes in the victim's browser after login.	6.1	More Details
CVE-2026-126495	MQTTX desktop through 1.13.3 contains a stored cross-site scripting vulnerability that allows attackers to inject script by publishing malicious MQTT topic names or payloads rendered unescaped in tooltips. Attackers controlling a broker or publishing to subscribed topics can execute script in the Electron renderer, which has nodeIntegration enabled, when victims hover Topic Tree or JSON tree nodes.	6.1	More Details
CVE-2026-121526	A url redirection to untrusted site ('open redirect') vulnerability in Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10 may allow an unauthenticated attacker to perform an open redirect attack via crafted HTTP requests.	6.1	More Details
CVE-2026-129484	Kroki before 0.36.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject scripts via unvalidated svg-color-dark-scheme and svg-color-light-scheme options. Attackers can craft a GET /goat/svg URL whose option value closes the SVG style element, executing JavaScript in the Kroki origin when victims open it.	6.1	More Details
CVE-2026-126393	SiYuan before 3.8.10 contains a server-side request forgery vulnerability in the skill-install download path because fetchBytes performs only a parse-time hostname check instead of using ssrfSafeClient. Attackers can supply a skill URL via the MCP skill install action that redirects or DNS-rebinds to loopback addresses, reaching internal services and metadata endpoints.	6.1	More Details
CVE-2026-9870	IBM Cyber Fraud 1.0.0 through 1.1.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2026-15785	The Joinchat – Enhanced "click to chat" plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via '{HREF}' Dynamic Variable via Query Parameter Name in all versions up to, and including, 6.3.1 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 an administrator has configured a telephone number and included the {HREF} dynamic variable in the Call-to-Action text.	6.1	More Details
CVE-2026-105154	Cross-Site Request Forgery (CSRF) in the Planet feed aggregator administration of Apache Roller 4.0 through 6.1.6 allows an unauthenticated attacker to make the Roller server fetch a URL the attacker chooses, including internal addresses, by inducing a logged-in global administrator to open a crafted web page. The action that adds a Planet subscription can be triggered cross-site; in recent releases it accepts GET requests, which Roller's CSRF token check does not cover. The action fetches the supplied URL and saves the subscription, and any fetched content that parses as a feed is then published without authentication in the aggregated Planet feed. The Planet aggregator is enabled by default. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which requires POST requests with a valid CSRF token for Planet administration changes and turns the Planet aggregator off by default.	6.1	More Details
CVE-2026-114468	IBM App Connect Operator and App Connect Enterprise Certified Containers Operands could allow an attacker with the ability to run HTTP calls within the running container to can make administrative calls to a running IntegrationRuntime.	6.0	More Details
CVE-2026-128070	Nuxt is an open-source web development framework for Vue.js. From 3.5.0 until 4.6.4, Nuxt can choose a parent directory as the default workspaceDir in either of two cases: a stray parent lockfile when the project is outside a Git repository and has no workspace file above it, or a parent pnpm or Deno settings file that does not declare packages or a workspace, including when the project is inside a Git repository. When the development server is reachable from an untrusted network, Vite permits /_nuxt/@fs/ requests beneath that widened directory, allowing unauthenticated clients to read files such as credentials and SSH keys. The issue affects the development server only; production builds and projects whose parent directories contain no qualifying files are unaffected. This issue is fixed in version 4.6.4.	5.9	More Details
CVE-2026-75488	Cudy TR3000 before 2.5.42 contains a stack buffer overflow vulnerability in the CWMP client that allows a malicious ACS to corrupt stack memory via oversized credentials. Attackers controlling the ACS can send Username and Password values up to 256 bytes in TR-069 Download or Upload requests, overflowing 128-byte stack buffers and crashing the CWMP process.	5.9	More Details
CVE-2026-126398	vLLM from 0.28.0 before 0.30.0 contains a reachable assertion vulnerability in GPUModelRunner._init_xdrope_positions that allows remote attackers to crash the engine by submitting embeddings-only requests. Attackers can send a /v1/completions request containing only prompt_embeds to XD-RoPE models with --enable-prompt-embeds, terminating the EngineCore and API server for all clients.	5.9	More Details
CVE-2026-92735	HashiCorp Vault and Vault Enterprise are vulnerable to an issue in the integrated storage join process that may allow an unauthenticated attacker with network access to a new, uninitialized node to cause that node to send credentials from its server environment to an attacker-controlled server. This vulnerability (CVE-2026-92735) is fixed in Vault Community Edition 2.2.2 and Vault Enterprise 2.2.2, 1.21.14, and 1.19.25.	5.9	More Details
CVE-2026-	Stack-based buffer overflow vulnerability in Apache HTTP Server's mod_vhost_alias (after CVE-2026-63292) This	5.9	More

109163	issue affects Apache HTTP Server: 2.4.69.		Details
CVE-2026-75493	Cudy TR3000 before 2.5.42 contains a stack buffer overflow vulnerability in an obuspa getter for the TR-098 WLANConfiguration KeyPassphrase parameter, which copies the stored value with strcpy() into a 4,096-byte stack buffer without a length check. A malicious or compromised ACS can set a 5,000-byte passphrase via SetParameterValues, and a later read of the parameter overflows the buffer and crashes obuspa, causing denial of service.	5.9	More Details
CVE-2026-126440	OpenEMR before 8.5.0 contains a missing authorization flaw in the Care Coordination CCDA and CCR import controllers, which move a document named by the document_id parameter into the import category without checking access to the source document. Authenticated non-administrators with Care Coordination access can recategorize protected patient documents and then download them through normal ACL-checked retrieval.	5.9	More Details
CVE-2026-128117	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to versions 2.70.4 and 3.1.1, the reroute hook could rewrite an invalid percent-encoded pathname into a valid route and reach a comparison that decoded the original malformed pathname outside the guarded decoding operation. The resulting unhandled URIError could crash an adapter-node server and deny service to other requests. This issue is fixed in 2.70.4 and 3.1.1.	5.9	More Details
CVE-2026-126432	OpenEMR before 8.5.0 contains an improper authorization vulnerability in interface/orders/list_reports.php that allows read-only users to transmit lab orders because the patients/med check ignores write permission. Authenticated attackers can submit form_xmit with arbitrary procedure order IDs to send HL7 orders containing SSNs, insurance, and diagnoses to laboratories and mark them transmitted.	5.9	More Details
CVE-2026-126346	basic-ftp is an FTP client for Node.js. Prior to 6.2.3, FTPContext.send() throws when a command contains carriage return, line feed, or NUL characters, but calls made from response handlers execute synchronously inside the control socket's data event without an exception boundary. In Client.login(), an attacker-influenced password reaches the PASS command after a server sends a 331 response, and in a resumed download an attacker-influenced remote path reaches the RETR command after a 350 response to REST. The resulting exception does not reject client.access() or downloadTo(), escapes ordinary promise error handling, and terminates the Node.js process, while the validation guard still prevents command injection. This issue is fixed in version 6.2.3.	5.9	More Details
CVE-2026-15201	An improper certificate validation vulnerability in the Support Form in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows man-in-the-middle attackers to read arbitrary files and write specific files during support form submission.	5.9	More Details
CVE-2026-128119	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From version 2.60.1 until 3.1.1, applications using the experimental remote functions flag could assign the same generated identifier to separate non-exported query.batch functions. When those private functions shared a request batch, arguments intended for one function could be passed to another function, causing unexpected cross-function processing and possible disclosure of function arguments. This issue is fixed in 3.1.1.	5.9	More Details
CVE-2026-126433	OpenEMR before 8.5.0 contains an improper authorization vulnerability in interface/drugs/dispense_drug.php, which checks only for admin/drugs view permission instead of write permission before dispensing medication. Authenticated users with read-only drug administration access can send GET requests with drug_id, quantity, fee, and encounter parameters to create false dispensing records and decrement inventory.	5.9	More Details
CVE-2026-128030	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains an insufficient session expiration vulnerability because Mage_Api_Model_Session::_renewBySessId() never checks api_user.is_active and REST OAuth authorization never checks whether the admin user is active. Attackers holding an existing SOAP/XML-RPC session or OAuth access token retain API access after deactivation or API key rotation, reading and modifying customer, order and catalog data.	5.9	More Details
CVE-2026-126444	OpenEMR before 8.5.0 contains a missing authorization vulnerability in the Ensora eRx integration that allows authenticated staff without patients/rx permission to access prescription data by directly requesting eRx.php. Attackers can expose selected patients' demographic, medication, and allergy data in the vendor XML and trigger eRx synchronization state changes.	5.9	More Details
CVE-2026-129319	create-ecdh is a browserifiable implementation of Node.js crypto.createECDH. In versions 4.0.4 and below, the JavaScript implementation (browser.js, used by browser bundlers and on Node.js versions without a working native crypto.createECDH) did not validate peer public keys in ECDH.prototype.computeSecret or ECDH.prototype.setPublicKey. The peer point was multiplied by the local private key without checking that it was on the configured curve or in its prime-order subgroup. An attacker who can submit public keys to a party that reuses a static private key can perform an invalid-curve or small-subgroup attack and recover the private key modulo small factors, eventually recovering the full key via the Chinese Remainder Theorem. For the ed25519 and curve25519 curves, low-order points were also accepted, which could force a predictable shared secret. On modern Node.js, create-ecdh re-exports the native implementation, which is not affected. This issue is fixed in version 4.0.5.	5.9	More Details
CVE-2026-124015	XWEB EVO 5.6.2 through 5.8.8 contains an authentication bypass vulnerability that allows unauthenticated attackers to set the password of any account flagged must-reset-at-next-login by exploiting missing session validation in the users.lua update_password action. Attackers can reset the password of newly onboarded operator accounts, clearing the password_expiration flag and gaining an immediately usable authenticated	5.9	More Details

	foothold on the system. This product line reached it's end of service date in March 2026.		
CVE-2026-128024	FrankenPHP before 1.13.0 contains a denial of service vulnerability in goArray() that allows remote attackers to abort the server process via arrays with null integer-keyed elements. Attackers can send crafted JSON passed to frankenphp_log() or returned from worker callbacks, triggering an unrecovered cgo panic that terminates every vhost and in-flight request.	5.9	More Details
CVE-2026-126936	Zipline before 4.7.0 contains a race condition vulnerability that allows users to bypass invitation usage limits, upload storage quotas, and shortened-URL quotas through concurrent requests. Attackers can send overlapping registration, upload, or URL creation requests that pass checks against stale state, creating extra accounts and exceeding administrator-configured resource quotas.	5.9	More Details
CVE-2026-128020	FrankenPHP before 1.13.2 contains an uncontrolled recursion vulnerability in its PHP-to-Go array converter that fails to detect circular references in PHP arrays. Passing a self-referential array to frankenphp_log() or returning one from a worker callback triggers a fatal Go stack overflow, terminating the entire server process.	5.9	More Details
CVE-2026-127099	A flaw was found in SSSD's conversion of X.509 certificate RSA public keys to SSH keys. Missing size checks before copying RSA components into fixed-size stack buffers can cause a stack buffer overflow. An attacker able to supply a certificate with oversized RSA components that passes the configured certificate checks can cause denial of service and corrupt SSH responder memory.	5.9	More Details
CVE-2026-119529	The Gravity Forms WordPress plugin before 3.2.2 does not properly restrict the file types that unauthenticated users can upload through its chunked file upload feature, allowing them to read server environment variables and the contents of files within the web root on servers configured to parse Server-Side Include documents, such as Apache with SSI enabled.	5.9	More Details
CVE-2026-129162	Dromara free-fs 2.0.1 through 2.3.1 contains a missing authentication vulnerability in FileStreamController.preview that allows unauthenticated attackers to download stored files. Attackers who obtain a file ID from share listings or preview links can request /api/file/stream/preview/{fileId} to download any user's or workspace's files.	5.9	More Details
CVE-2026-126906	Race condition in Extensions in Google Chrome on on Mac prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to obtain sensitive information via crafted network traffic. (Chromium security severity: High)	5.9	More Details
CVE-2026-128121	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to @sveltejs/adapter-vercel 6.3.5 and 7.0.2 and @sveltejs/adapter-static 3.0.11 and 4.0.1, an attacker-influenced link crawled during prerendering could be emitted into the generated Vercel routing configuration without escaping regular-expression metacharacters. The configuration could consequently interpret the path as regular-expression syntax, match unintended application paths, and expose content or behavior outside the intended path. This issue is fixed in @sveltejs/adapter-vercel 6.3.5 and 7.0.2 and @sveltejs/adapter-static 3.0.11 and 4.0.1.	5.9	More Details
CVE-2026-126287	NocoDB before 2026.06.2 contains a race condition vulnerability in oauth-token.service.ts that allows attackers to reuse a refresh token by presenting it concurrently during non-atomic rotation. Attackers holding a captured refresh token can race the legitimate client to obtain their own access and refresh tokens, retaining scoped access without triggering reuse detection.	5.9	More Details
CVE-2026-128123	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From version 5.5.7 until versions 5.5.8 and 6.0.1, , @sveltejs/adapter-node can attempt to add a header to an immutable request in a context that causes the server to crash, denying service to any other requests routed to that server. This issue is fixed in 5.5.8 and 6.0.1.	5.9	More Details
CVE-2026-97054	For HTTP/1 servers, when MaxBytesReader's limit is exceeded, "Connection: close" header is automatically set without synchronization, which might race with another header being set explicitly in the server handler. As a result, an HTTP/1 server that utilizes MaxBytesReader or MaxBytesHandler can crash due to runtime panic if its handler reads the request body concurrently with writing the response header.	5.9	More Details
CVE-2026-126420	OpenEMR before 8.5.0 contains a missing authorization vulnerability in the FaxSMS module's utility.php that allows read-only demographics users to create patient charts. Attackers can submit the form_create request with chosen identity fields to create fictitious or duplicate patients with employer, history, and insurance records.	5.9	More Details
CVE-2026-126351	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. Prior to 2.9.1, Addressable::URI.normalize_path repeatedly scans and rewrites paths while removing only one nested dot segment per pass, producing quadratic work. URI#normalize, URI#normalized_path, URI#join, URI#==, and URI#=== inherit the behavior, so processing a sufficiently long attacker-controlled URI can consume a worker thread and cause denial of service on every Ruby implementation. URI.parse alone and code that never normalizes, compares, or joins untrusted URIs are unaffected. This issue is fixed in version 2.9.1.	5.9	More Details
CVE-2026-126352	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.3.0 until 2.9.1, URI templates with several variables in one expression or several adjacent expressions generate ambiguous regular expressions. Affected forms include multi-variable expressions using operators other than plus and number sign, large plus or number-sign expressions, and adjacent single-variable expressions. Template#match or Template#extract can backtrack polynomially or exponentially on attacker-	5.9	More Details

	controlled URIs, causing denial of service on MRI Ruby before 3.2 and JRuby, with the large plus and number-sign form also affecting MRI Ruby 3.2 and TruffleRuby 40.0. URI parsing and Template#expand are unaffected. This issue is fixed in version 2.9.1.		
CVE-2026-129164	Dromara free-fs 2.0.1 through 2.3.1 contains an authorization bypass vulnerability that allows attackers to access code-protected shares because share codes are enforced only client-side. Attackers knowing a share ID can call the share items and download endpoints to list and download files without the code, even on preview-only shares.	5.9	More Details
CVE-2026-19194	The HashiCorp cap JWT validation library before version 0.14.0 is vulnerable to a claims validation bypass that may cause downstream applications to make authorization decisions using claim values different from those validated. Exploitation requires attacker-controlled claims in a JWT signed by a key trusted by the application. This vulnerability (CVE-2026-19194) is fixed in cap 0.14.0.	5.9	More Details
CVE-2026-126353	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.3.0 until 2.9.1, URI template expressions containing several exploded variables generate ambiguous regular expressions that can divide a run of members among the variables in polynomially many ways. Template#match or Template#extract processing of an attacker-controlled URI can therefore consume a thread and cause denial of service. The flaw affects MRI Ruby before 3.2 and JRuby, TruffleRuby 40.0, and plus or number-sign expressions on MRI Ruby 3.2. MRI Ruby 3.3 and later, URI parsing, and Template#expand are unaffected. This issue is fixed in version 2.9.1.	5.9	More Details
CVE-2026-128122	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From version 4.7.0 until versions 7.2.10 and 8.0.2, @sveltejs/adapter-cloudflare allowed an attacker-influenced link crawled during prerendering to place whitespace, control characters, wildcards, or placeholders into a prerendered redirect path. The adapter wrote those paths into the Cloudflare _redirects output without output-context validation, allowing a path to create unintended routing rules that could redirect or expose requests beyond the intended prerendered route. This issue is fixed in 7.2.10 and 8.0.2.	5.9	More Details
CVE-2026-126350	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.3.0 until 2.9.1, URI template expressions using the explode modifier with the slash, dot, semicolon, question-mark, or ampersand operators generate ambiguous regular expressions. When Template#match or Template#extract processes an attacker-controlled URI beginning with the operator's leading character, optional member separators allow catastrophic backtracking and denial of service on MRI Ruby before 3.2 and JRuby. Addressable 2.9.0 incompletely remediated the earlier template issue because its tests did not reach these operator-prefixed paths. URI parsing and Template#expand are unaffected. This issue is fixed in version 2.9.1.	5.9	More Details
CVE-2026-129485	Kroki before 0.36.0 contains a server-side request forgery vulnerability in the BlockDiag family of engines that allows unauthenticated attackers to make server requests via node icon and background attributes. Attackers can send crafted diagrams to POST /blockdiag/svg or sibling endpoints to query internal services or cloud metadata and read local image files from the server.	5.8	More Details
CVE-2026-126311	OpenBao before 2.6.5 and 2.7.x before 2.7.2 does not neutralize wildcard characters in SSH certificate principals rendered from unvalidated external token metadata via identity templates in the SSH secrets engine. Attackers controlling that metadata, typically through a compromised identity provider, can inject '*' to obtain SSH certificates valid for multiple hosts or users.	5.8	More Details
CVE-2026-128080	OpenTelemetry JavaScript is the OpenTelemetry JavaScript client. From 0.204.0 until 0.222.0, @opentelemetry/instrumentation-http writes the raw query string from incoming HTTP requests to the url.query server-span attribute without applying the redactedQueryParams protection used for outgoing spans. Services receiving signed URLs or other credentials in query parameters can therefore export still-valid secrets to tracing backends, where observability infrastructure and users with span-read access may read them. The redactedQueryParams option does not protect incoming spans in affected versions. This issue is fixed in version 0.222.0.	5.8	More Details
CVE-2026-65950	A path traversal vulnerability in the ZIP extraction logic of Lenovo XClarity Essentials OneCLI 5.5.0 for Linux could allow an attacker to write arbitrary files with the privileges of the OneCLI process by convincing a user to process a specially crafted ZIP-based update package.	5.8	More Details
CVE-2026-65951	A path traversal vulnerability in the TAR.GZ extraction logic of Lenovo XClarity Essentials OneCLI 5.5.0 for Linux could allow an attacker to write arbitrary files with the privileges of the OneCLI process by convincing a user to process a specially crafted TAR.GZ update package.	5.8	More Details
CVE-2026-126944	Zipline before 4.6.1 contains a path traversal vulnerability in LocalDatasource that allows SUPERADMIN users to read or delete files outside the upload directory by importing records with traversal filenames. Attackers can trigger the unchecked range-read path with byte-range requests or set expired deletion times to delete files accessible to the Zipline process.	5.7	More Details
CVE-2026-123065	When a release was edited, the files of the attachments to remove were deleted by the identifiers submitted in the form rather than by the attachments verified to belong to the release. A user with write access to the releases of any repository, including their own, could submit a crafted identifier that resolves to the stored file of another attachment and delete it, provided they know that attachment's UUID. The attachment record stayed, so downloads of the affected issue, comment or release file failed. Release edits now only delete the files of attachments that belong to the release.	5.7	More Details

CVE-2026-92241	The AVRCP browsing channel's L2CAP receive-buffer callback, browsing_avrcp_l2cap_alloc_buf() in subsys/bluetooth/host/classic/avrcp.c, allocated from the shared avctp_browsing_rx_pool with K_FOREVER. L2CAP invokes that callback from the Bluetooth RX work queue thread (bt_workq, "BT RX WQ"), both for the head buffer of a new SDU and — through l2cap_br_alloc_frag() and net_buf_append_bytes() — for every further fragment of a reassembled SDU. That same thread is the only context that ever releases these buffers, after bt_l2cap_br_recv_seg() delivers a completed SDU and calls net_buf_unref(), so a wait taken there can never be satisfied. The pool holds CONFIG_BT_MAX_CONN + 1 buffers of CONFIG_BT_AVRCP_BROWSING_L2CAP_MTU bytes (two buffers of 339 bytes in the default configuration). A connected browsing peer can drain it because bt_l2cap_br_recv_seg() in subsys/bluetooth/host/classic/l2cap_br.c accepts the SDU length declared in an SAR_START segment without bounding it by br_chan->rx.mtu: a peer that announces a large SDU and then streams continuation segments forces one pool buffer per segment-worth of data. Once the pool is empty the next allocation blocks forever inside the callback. Triggering the flaw requires a build with CONFIG_BT_CLASSIC and the experimental CONFIG_BT_AVRCP_BROWSING option, an application that registers AVRCP callbacks, and a BR/EDR peer that has established the AVRCP control channel and then the browsing channel, which requires an encrypted (paired) link. No malformed packet is needed — a few hundred bytes of ordinary segmented L2CAP traffic suffice. The consequence is a permanent hang of the whole Bluetooth host, not just of AVRCP: the blocked thread drains bt_dev.rx_queue for all HCI ACL data and low-priority events and also runs the host's internal work items, so all connections stop being serviced and the state is unrecoverable without a reboot. There is no memory-corruption or information-disclosure component. The fix allocates with K_NO_WAIT, so an empty pool now yields a local-busy indication or a channel disconnect that the application can recover from.	5.7	More Details
CVE-2026-129092	CCC Attestation SIG attested-tls-poc through commit 731ca82 contains a time-of-check time-of-use vulnerability because Evidence is appraised only once during the TLS handshake, without post-handshake re-attestation. Attackers with local access to the attesting endpoint can alter workload code, data, configuration, or attached devices like GPUs while peers keep trusting the original Evidence.	5.7	More Details
CVE-2026-111434	Use of Externally-Controlled format string vulnerability in openEuler iSulad on Linux. This vulnerability is associated with program file src/daemon/modules/image/oci/oci_load.c. This issue affects iSulad: through 2.1.6. When the iSulad daemon performs container lifecycle operations (such as create, start, exec, stop, etc.) through the isula runtime (shim), the daemon reads the stderr output of the shim process via a pipe for error information display. If the buffer contains format specifiers such as %s, %x, or %n, it may trigger a format string vulnerability, potentially leading to information leakage, denial of service, or the risk of arbitrary writes.	5.6	More Details
CVE-2026-129490	littlefs through 2.11.3, when built with LFS_MIGRATE, contains a type confusion vulnerability in lfs_dir_traverse() that treats a stack lfs_diskoff struct as an lfs_attr array. Attackers can supply a crafted littlefs v1 image whose metadata is read as LFS_FROM_USERATTRS during migration, causing out-of-bounds stack reads and process crashes.	5.5	More Details
CVE-2026-127101	A flaw was found in SSSD's PAM responder. A local attacker can send an authentication request without first negotiating the client protocol version. The responder dereferences a NULL protocol-version pointer and crashes, disrupting SSSD-backed authentication. Repeated crafted requests can sustain the denial of service.	5.5	More Details
CVE-2026-124742	A flaw was found in BusyBox. The volume identification component fails to properly validate cluster parameters when analyzing specially formatted FAT filesystems. An attacker able to present a crafted storage device or disk image can trigger a divide-by-zero condition when partition scanning utilities inspect the volume. This issue causes the probing utilities to crash unexpectedly, resulting in a Denial of Service (DoS) that can disrupt device discovery and system boot operations.	5.5	More Details
CVE-2026-127100	A flaw was found in SSSD's PAM responder on builds with the JSON PAM extension enabled. A local attacker can submit a crafted authentication request containing a non-string OAuth2 code value. Missing JSON type validation leads to a NULL pointer dereference, terminating the PAM responder and disrupting SSSD-backed authentication.	5.5	More Details
CVE-2026-128885	A flaw was found in D-Bus. In configurations where the daemon falls back to using the Unix select() mechanism for event monitoring, it does not verify whether file descriptor numbers exceed allocated limits. A local attacker can exploit this flaw by opening a large number of concurrent connections to trigger an out-of-bounds write on the stack. This can cause the daemon to crash, resulting in a Denial of Service (DoS).	5.5	More Details
CVE-2026-126831	A flaw was found in cpio. A local user can cause a Denial of Service (DoS) by triggering a stack-based buffer overflow when creating archives in tar or ustar formats. When archiving files owned by users or groups with names exceeding 32 characters, cpio copies these names into fixed-size memory without verifying their length. This unbounded copy corrupts stack memory and causes the application to crash.	5.5	More Details
CVE-2026-110330	A flaw was found in abrt. abrt-server trusts a client-supplied PID when creating problem dumps over abrt.socket and, running as root, copies that process's /proc data (including environ) into a dump directory owned by the connecting unprivileged user. This allows a local attacker to read environment variables and related metadata of other users' or root processes when abrtd is running.	5.5	More Details
CVE-2026-118535	A repository registered by its owner as a source of scoped workflows kept that registration when it was transferred to another owner. The new owner could then change the workflows in the transferred repository, and they kept running in the previous owner's repositories with access to their Actions secrets and job tokens. A transfer now removes the owner-level registrations of the repository, and registrations whose source repository no longer belongs to the registering owner are ignored.	5.5	More Details

CVE-2026-124743	A flaw was found in BusyBox. When processing filesystem metadata, the volume identification component does not properly validate header values in HFS+ filesystems. An attacker able to attach a storage device or supply a specially crafted filesystem image can trigger an application crash, resulting in a Denial of Service (DoS) and preventing device resolution.	5.5	More Details
CVE-2026-116412	Dell PowerStore contains an insecure-file-permissions vulnerability. A local low-privileged attacker could exploit this vulnerability to disclose administrative credentials.	5.5	More Details
CVE-2026-129264	A security vulnerability has been detected in sox_ng up to 14.8.1. Affected by this issue is the function read_samples_voc of the file src/voc.c of the component VOC Decoder. Such manipulation leads to out-of-bounds write. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The name of the patch is 0b40408b. A patch should be applied to remediate this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	5.5	More Details
CVE-2026-126838	A MongoDB Rust Driver component that holds client-side field level encryption settings includes key management service credential material in its diagnostic formatting output without redaction. An application that records or displays this formatted output may place that material where a party with read access to the application's diagnostic output can see it, which may result in unintended disclosure of key material.	5.5	More Details
CVE-2025-71468	GPAC before 26.02.0 contains a NULL pointer dereference vulnerability in gf_dash_group_get_audio_channels() in src/media_tools/dash_client.c that allows attackers to crash applications via crafted DASH manifests. Attackers can supply an MPD whose AudioChannelConfiguration element omits schemeIdUri or value, crashing MP4Box or GPAC DASH clients and causing denial of service.	5.5	More Details
CVE-2026-109096	Incorrect handling of negative returns from ddQueryImageAttributes() when processing XvPutImage requests in X.Org xwayland before 24.1.15 and X Server before 21.1.26 could be used by authenticated X clients to crash the X server.	5.5	More Details
CVE-2026-91872	Dell Ansible Storage for PowerStore, versions prior to 3.9.0,contains an Insertion of Sensitive Information into Log File vulnerability in the configuration module. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	5.5	More Details
CVE-2026-86363	Dell Live Optics Collector, versions prior to 27.3.13.330 contains a Generation of Predictable IV with CBC Mode vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	5.5	More Details
CVE-2026-128240	GPAC through 26.07.0 contains a use-after-free vulnerability in gf_sg_proto_del() in src/scenegraph/vrml_proto.c because gf_sg_reset() frees unregistered prototypes still referenced by scene commands. Attackers can supply a crafted XMT/BT scene declaring prototypes via commands, processed by MP4Box -chap, to trigger freed memory access and crash the process.	5.5	More Details
CVE-2026-129477	Assimp through 6.0.6 contains a path traversal vulnerability in the glTF and glTF2 importers that allows attackers to read local files via crafted buffers[].uri values. Attackers can supply glTF models with '..' segments or absolute paths in buffer URIs to load files like /etc/passwd into imported mesh vertex data.	5.5	More Details
CVE-2026-128239	GPAC through 26.07.0 contains a NULL pointer dereference vulnerability in the MPEG-4 Form spatial-constraint handlers in src/compositor/mpeg4_form.c that lets attackers crash the process via unchecked group lookups. Attackers can supply a crafted XMT scene whose Form constraints reference a non-existent group, crashing tools like MP4Box during chapter import for denial of service.	5.5	More Details
CVE-2026-91876	Dell OpenManage Ansible Modules, versions 2.0.4 through 10.0.3, contains an Improper Restriction of XML External Entity Reference vulnerability in the XML parsing component. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	5.5	More Details
CVE-2026-129479	Assimp through 6.0.6 contains an integer overflow vulnerability in OgreBinarySerializer::ReadSubMesh that allows attackers to crash applications by supplying crafted Ogre binary .mesh files. Attackers can set a large index count so the 32-bit buffer size wraps, causing a segmentation fault in aiMesh::~aiMesh() during scene teardown.	5.5	More Details
CVE-2025-71466	GPAC before 26.02.0 contains a NULL pointer dereference vulnerability in m2tsdmx_update_sdt() in src/filters/dmx_m2ts.c that allows attackers to crash the MPEG-2 TS demuxer. Attackers can supply a crafted .ts file with an invalid service descriptor leaving service or provider names NULL to crash MP4Box and cause denial of service.	5.5	More Details
CVE-2026-127093	Rustrak before 0.26.0 contains a server-side request forgery vulnerability that allows users with integrations update permission to send requests to arbitrary destinations by supplying routing_override.url to POST /api/integrations/{id}/test. Attackers can target loopback, private-network and cloud metadata addresses with custom headers and redirects followed, reading non-2xx response bodies returned in the API response.	5.5	More Details
CVE-2025-71467	GPAC before 26.02.0 contains a NULL pointer dereference vulnerability in gf_node_get_field_by_name() in src/scenegraph/base_scenegraph.c that lets attackers crash applications. Attackers can supply a crafted XMT scene referencing a never-created node to crash MP4Box or GPAC scene loader applications, causing denial of service.	5.5	More Details

CVE-2025-71469	GPAC before 26.02.0 contains a type confusion vulnerability in ctxload_process() that passes non-object descriptors to ODS_SetupOD() without checking the descriptor tag. Attackers can supply a crafted XMT file with a URL-bearing descriptor that crashes MP4Box or other GPAC-based applications in gf_scene_ns_connect_object(), causing denial of service.	5.5	More Details
CVE-2026-91094	A directory traversal bug was discovered when unpacking 3.0 (quilt) source packages, where the packaging tarball could contain the quilt database directory (.pc) with attacker controlled symlinks, where that in combination with patches that would fail to apply, could be used to make the code used to restore the backup files to either modify or remove the files pointed to by the attacker controlled symlinks.	5.5	More Details
CVE-2025-71470	MicroQuickJS (mquickjs) before commit 99eed3f contains an out-of-bounds read vulnerability because JS_Call() raises exceptions during frame setup without updating ctx->sp and ctx->fp. Attackers can supply JavaScript that calls a non-function value, causing build_backtrace() to walk stale frame pointers and crash the engine for denial of service.	5.5	More Details
CVE-2026-124746	A flaw was found in BusyBox. An integer overflow occurs in the volume_id component when calculating buffer boundaries while probing filesystem metadata. An attacker can exploit this vulnerability by providing a specially crafted filesystem image on an attached storage device. When probed by utilities such as blkid, findfs, or mount, the application crashes, resulting in a Denial of Service (DoS) that prevents the system from resolving or mounting storage devices.	5.5	More Details
CVE-2026-110289	A user with the Organization Admin role could point the server or token URL of a Git Sync connection at a loopback or internal address, and Grafana would then send the connection's OAuth client secret and tokens, or requests signed with the GitHub App private key, to that address (server-side request forgery).	5.5	More Details
CVE-2026-128034	In gittuf before 0.18.0, verification of file protection rules uses the quoted, escaped pathnames that Git prints by default for files with special characters (for example non-ASCII characters) instead of the raw paths. Such paths do not match patterns like file:internal/*, so the files are treated as unprotected, and a user who is not authorized by a file protection rule can change a protected file whose name contains special characters and still pass verification.	5.5	More Details
CVE-2026-128035	In gittuf 0.10.0 through 0.17.0, the verification workflow does not load policy updates that are propagated from an upstream (controller) repository and recorded in the reference state log after the first entry being verified. Only the propagated policy in effect at the start of verification is applied, so later controller changes to global rules, such as threshold requirements and force-push blocks, are ignored and changes that these rules should block pass verification.	5.5	More Details
CVE-2026-116438	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0 , contains a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	5.4	More Details
CVE-2026-116453	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering and Unauthorized access.	5.4	More Details
CVE-2026-126564	Semantic MediaWiki 2.5.0 before 7.4.1 contains a stored cross-site scripting vulnerability in ValueFormatter::getFormattedSubject() that renders property label segments after a literal as unescaped markup. Users with page-edit rights can set a preferred property label containing an img onerror payload that executes when anyone, including administrators, views Special:Browse or the smwbrowse API.	5.4	More Details
CVE-2026-126560	Semantic MediaWiki 3.0.0 before 7.4.1 contains a stored cross-site scripting vulnerability in the DataTables integration that initialises author-written smw-datatable tables unchanged. Users with page-edit rights can add HTML entity-encoded markup in data-search or data-filter cell attributes, executing script in viewers' browsers including administrators.	5.4	More Details
CVE-2026-126498	WriteFreely before 0.17.3 contains a stored cross-site scripting vulnerability that allows authenticated authors to inject HTML by supplying a malicious post slug via the CreatePost API. The raw slug is concatenated into an anchor by augmentReadingDestination() for paid-shortcode posts, executing script for RSS/Atom feed readers, newsletter recipients and ActivityPub viewers.	5.4	More Details
CVE-2026-126567	Semantic MediaWiki 3.0.0 before 7.4.1 contains a stored cross-site scripting vulnerability in Special:Ask with the ElasticStore backend, allowing users with edit rights to inject script through unescaped native_result and score_set output. Attackers can store markup in a Text property or subobject name, then lure victims including administrators to a crafted Special:Ask link to execute script in their session.	5.4	More Details
CVE-2026-126569	Mbin 1.2.1 before 1.11.1 contains a stored cross-site scripting vulnerability in EmbedElement::buildDestructed() that renders nested Markdown image alt text and URL without HTML escaping. Authenticated users can embed HTML in the alt text of an image inside a link in entries, comments, posts, messages, or bios to run script in viewers' browsers.	5.4	More Details
CVE-2026-126382	n8n before 2.38.0 and 3.x before 3.0.1 contains a missing authentication vulnerability in the Asana Trigger that accepts a new webhook verification secret from any request carrying an X-Hook-Secret header. Unauthenticated attackers who know the webhook URL can replace the secret, send forged Asana events that pass signature verification, and trigger workflows with attacker-controlled data while genuine deliveries are rejected.	5.4	More Details

CVE-2026-128824	A flaw was found in Red Hat Quay. The v1 registry API error handler reflects the attacker-supplied image_id path segment in a response served as text/html, allowing a reflected cross-site scripting (XSS) attack. By tricking a user into visiting a specially crafted URL, a remote attacker can execute arbitrary JavaScript in the victim's browser within the Quay origin, potentially compromising the user's session.	5.4	More Details
CVE-2026-128359	When Gitea acts as an OAuth2 or OpenID Connect provider, the token endpoint did not check the state of the user. After an administrator deactivated an account or prohibited its sign-in, existing refresh tokens and unused authorization codes of that user could still be exchanged for new tokens, so applications that sign users in through Gitea kept them signed in. The token endpoint now refuses users who may not sign in, and token introspection reports their tokens as inactive.	5.4	More Details
CVE-2026-126369	Vvveb through 1.0.8.6 contains a stored cross-site scripting vulnerability that allows low-privilege author or vendor users to inject script by bypassing the regex blacklist in sanitizeHTML(). Attackers can save post or product content with unclosed event-handler tags or javascript: entities to execute script for anonymous visitors and admins, enabling session or CSRF-token theft.	5.4	More Details
CVE-2026-126371	Vvveb through 1.0.8.6 contains an SQL injection vulnerability in Admin_Auth_TokenSQL::update(), which interpolates admin_auth_token array keys into an INSERT column list without a column whitelist or backtick escaping. Authenticated admin-panel users can submit backtick-containing keys to the admin/auth-token save action to inject comments and column identifiers into the SQL statement.	5.4	More Details
CVE-2026-125434	Missing Authorization vulnerability in Webful Creations RepairBuddy computer-repair-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RepairBuddy: from n/a through 4.1235.	5.4	More Details
CVE-2026-120729	The popup shown when hovering an issue reference loaded its data from the path of the hovered link and inserted part of the response as HTML. A user who can post a comment or other rendered content could add a link that is displayed as an ordinary issue reference but points to a file in a repository they control, so that the popup inserted that file's content into the page of anyone hovering the link and ran script in the viewer's session. The popup now requests the issue by the owner, repository and index parsed from the link.	5.4	More Details
CVE-2026-126289	NocoDB before 2026.06.1 contains a CSV formula injection vulnerability in export.service.ts that writes record values and column titles beginning with formula characters into CSV exports without neutralization. Low-privileged collaborators, or unauthenticated users submitting a public form, can plant formulas that execute when a user opens the export in a spreadsheet application, potentially exfiltrating cell contents or invoking external commands.	5.4	More Details
CVE-2026-124408	Missing Authorization vulnerability in Arraytics WPCafe wp-cafe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPCafe: from n/a through 3.0.22.	5.4	More Details
CVE-2026-118587	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in all versions up to, and including, 11.18.0 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. This vulnerability is only exploitable when the site's configured video player is set to html5video, or when the media URL uses a .webm or .ogv extension, as these conditions are required to route the shortcode attributes through the vulnerable powerpressplayer_build_html5video() builder. Successful exploitation additionally requires an action by an editor — the attacker cannot trigger the vulnerability on their own.	5.4	More Details
CVE-2026-126376	Vvveb 1.0.8.4 through 1.0.8.6 contains an incomplete authorization fix that allows low-privilege authors and vendors to access other users' records by bypassing admin_id owner scoping. Attackers can supply filter[admin_id] to list drafts, invoke duplicate() on posts or products, or enumerate every vendor's digital-asset metadata.	5.4	More Details
CVE-2026-121770	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme VISeek viseek-easy-custom-search allows Cross Site Request Forgery.This issue affects VISeek: from n/a through 1.0.5.	5.4	More Details
CVE-2026-126389	n8n before 1.123.89 contains an authentication bypass vulnerability in the Chat Trigger that allows unauthenticated attackers to skip n8n User Auth through the setup GET webhook route in embedded chat mode. Attackers can send unauthenticated GET requests to the chat webhook URL to read named session conversation history or trigger workflows with attacker-supplied input.	5.4	More Details
CVE-2026-129155	DjangoBlog 2.0.0.0 through 2.1.0.0 contains a stored cross-site scripting vulnerability because the class_filter comment sanitizer passes event-handler attributes on span, div, pre and code tags. Authenticated commenters can post a div with autofocus and onfocus attributes, executing script without interaction for every visitor, including administrators.	5.4	More Details
CVE-2026-116427	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	5.4	More Details
CVE-	An improper neutralization of input during web page generation vulnerability in the Audio Player in Synology		

2026-13656	DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write specific files.	5.4	More Details
CVE-2026-126456	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability in the Fee Sheet notecodes field, which is escaped with the wrong context. Attackers with clinician access can inject a payload that breaks out of the single-quoted value attribute and executes in higher-privileged users' browsers.	5.4	More Details
CVE-2026-129428	Pulse from 5.0.17 before 6.8.0 contains a missing authorization vulnerability in the /api/ai/approvals endpoints that allows authenticated viewer-level users to manage approval requests. Attackers can list pending requests to expose proposed commands and targets, and approve or deny other users' requests, altering decision and audit state.	5.4	More Details
CVE-2026-129430	Axeloz Filesharing before 2.14.3 contains a stored cross-site scripting vulnerability that allows authenticated users to inject script by storing raw HTML or javascript: Markdown links in bundle descriptions. Recipients viewing the public bundle preview page execute the script via Alpine x-html, letting attackers steal the owner_token from localStorage and issue owner-scoped requests against victim bundles.	5.4	More Details
CVE-2026-125787	Missing Authorization vulnerability in ExpressTech Quiz And Survey Master quiz-master-next allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Quiz And Survey Master: from n/a through 11.3.0.	5.4	More Details
CVE-2026-127236	An argument injection vulnerability exists in the ad-hoc RRD graph feature of multiple versions of OpenNMS Meridian and Horizon. The ad-hoc graph endpoint (GET /graph/graph.png?adhoc=true) copies request parameters into the rrdtool command line without validation. A low-privileged authenticated user (ROLE_USER or ROLE_DASHBOARD) can insert extra rrdtool arguments. An injected --daemon argument makes the server connect to an attacker-chosen address, which is a server-side request forgery. An injected DEF statement reads a local RRD file by absolute path. The command runs through exec with an argument array and no shell, so arbitrary operating system command execution is not possible. The fix validates the ad-hoc graph parameters against allowlists. The solution is to upgrade to Meridian 2024.3.15, 2025.0.12, 2026.0.2 and Horizon 36.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	5.4	More Details
CVE-2026-127115	The BuddyForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'buddyforms_form_content' parameter in all versions up to, and including, 2.10.6 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 is exploitable when a form configured with the public_submit option is published — a condition met by the plugin's bundled Post Simple template out of the box.	5.4	More Details
CVE-2026-63173	Omnispace Agora Project through 26.10.0 contains a broken access control vulnerability in which the isAutor() function in MdlObject.php grants accessRight=3 based solely on object authorship without verifying the user still belongs to the object's space. Attackers who were previously members and authored objects can retain unauthorized read access to space objects even after being removed from the space, leading to persistent information disclosure.	5.4	More Details
CVE-2026-129172	EdgeEver 1.9.0 before 2.13.0 contains a stored cross-site scripting vulnerability in the backup restore endpoint PUT /api/v1/restores/json/resources/:id, which accepts a resource kind of image paired with a text/html MIME type without checking consistency. Authenticated members can share the note and send the public blob link to a victim, whose browser executes the script to mint a non-expiring API token granting read and write access to the victim's notes.	5.4	More Details
CVE-2026-129455	Zr.Admin.NET commit e6ceaf4 through commit eb9228a contains an insecure direct object reference vulnerability in FrontArticleController that allows authenticated users to change other users' article visibility and pin state. Attackers can send PUT /front/article/changePublic with their own UserId in the body to make private articles public, then read them anonymously via GET /front/article/{id}.	5.4	More Details
CVE-2026-129169	PMail 2.5.0 through 2.9.8 contains a stored cross-site scripting vulnerability that allows authenticated users to inject scripts by sending unsanitized HTML through /api/email/send. Attackers can embed event-handler payloads like img onerror that execute when administrators view the message, enabling privileged API calls such as password changes for account takeover.	5.4	More Details
CVE-2026-127207	Sendcloud for WooCommerce through 1.0.41 contains a missing authorization vulnerability that allows authenticated low-privileged users, including Subscribers, to access the sc_support_get and sc_support_save AJAX actions due to the absence of capability and nonce checks in SCCSP_Support_Controller. Attackers can call these wp_ajax_ handlers directly or via cross-site request forgery to disclose integration configuration data such as INTEGRATION_ID, SERVICE_POINT, CARRIERS, and MIN_LOG_LEVEL, and to modify the plugin's logging verbosity. This is an incomplete fix of CVE-2026-57760.	5.4	More Details
CVE-2026-126811	BookStack before 26.09.3 contains an incorrect authorization vulnerability that allows authenticated users to access other users' unpublished draft page images by checking only PageView permission without draft status. Attackers can read drawio data via the base64 endpoint or rename, replace, or delete draft images by sequential ID to disclose or tamper with unpublished work.	5.4	More Details

CVE-2026-126435	OpenEMR before 8.5.0 contains an improper authorization vulnerability in interface/orders/order_manifest.php, which checks patients/med without requiring write access or applying patient squad restrictions. Users with only patients/med view permission can request any order ID to read squad-restricted patient data and submit bn_save and form_omit parameters, without a CSRF token, to set do_not_send flags that suppress ordered lab procedures.	5.4	More Details
CVE-2026-126344	@hono/node-server allows running the Hono application on Node.js. From 2.0.0 until 2.1.6, the WebSocket upgrade path resolves a raw request-target beginning with // against a base URL built from the Host header, causing the WHATWG URL parser to treat the request-target as a network-path reference and replace the host in c.req.url. Routing still uses the local WebSocket path, so an application that compares the Origin header with the origin of c.req.url, including checks implemented with csrf(), compares an attacker's origin with itself and accepts the connection. A page on another site can consequently open a WebSocket with the victim's cookies and read and send messages when the application uses upgradeWebSocket and trusts the host in c.req.url. Ordinary HTTP requests are not affected. This issue is fixed in version 2.1.6.	5.4	More Details
CVE-2026-114452	The Membership Plugin WordPress plugin before 4.0.6 does not verify that the membership referenced in a saved-card payment request belongs to the user making it, allowing subscriber-level members to disclose another member's Stripe payment client secret and attach a payment method of their choosing to another member's pending payment.	5.4	More Details
CVE-2026-126697	The Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 was distributed with a hidden update mechanism that fetched Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 updates from its author's own server instead of WordPress.org, which was used to push a backdoored build to sites, allowing the attacker controlling that server to inject arbitrary content into pages and to deliver arbitrary code to affected sites. Version 5.2.1, as published on WordPress.org, bundled the Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 Update Checker library (updater/ directory) configured to poll https://anadnet.com/updates/?action=get_metadata&slug=quick-pagepost-redirect-Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4. In March 2021 that server delivered a modified 5.2.3 build, different from the 5.2.3 later published on WordPress.org, which kept the update channel and added a the_content filter that, for logged-out visitors on single posts and pages, fetched content from https://w.anadnet.com/bro/3/ (passing the site host, request URI and visitor User-Agent) and prepended the response to the post (observed serving SEO spam links to search engine crawlers). Because the version string matched a later WordPress.org release, affected sites were not offered a clean update until 5.2.4. Indicators of compromise: - Outbound requests to anadnet.com or w.anadnet.com - An updater/ directory (Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 Update Checker, Puc v4p10) inside wp-content/Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4/quick-pagepost-redirect-Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4/ - The strings filter_the_content_in_the_main_loop, ppr_pro, QQQEND or w.anadnet.com in page_post_redirect_Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4.php - page_post_redirect_Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4.php with MD5 ad717da18cf8a2b69899c0d7dafee05a (tampered 5.2.3) Remediation: remove the Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 (it has been closed on WordPress.org), or at minimum reinstall the clean 5.2.4 from WordPress.org, delete any leftover updater/ directory, verify the files with "wp Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4 verify-checksums quick-pagepost-redirect-Quick Page/Post Redirect Plugin WordPress plugin before 5.2.4", clear the opcode cache, and treat any site that ran the tampered build as potentially compromised.	5.4	More Details
CVE-2026-19833	A missing authorization vulnerability in the ACL API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write specific files.	5.4	More Details
CVE-2026-129163	Dromara free-fs 2.0.1 through 2.3.1 contains a stored cross-site scripting vulnerability that allows registered users to run script by uploading HTML files served inline as text/html. Attackers can send a victim the /api/file/stream/preview/{fileId} link to execute script in the application origin, calling /apis endpoints to expose the victim's files and account.	5.4	More Details
CVE-2026-81557	An improper neutralization of input during web page generation vulnerability in the DSMNotify in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write specific files.	5.4	More Details
CVE-2026-16237	Improper protection in PostgreSQL INSERT ... ON CONFLICT on auto-updatable views allows an attacker having INSERT and UPDATE privileges on the view to read and modify every row in the view's base table, via iterated INSERT ... ON CONFLICT DO UPDATE. This bypasses the view's WHERE condition, whether or not the view is a security_barrier view. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	5.4	More Details
CVE-2026-110194	IBM ContextForge MCP Gateway 1.0.0 through 1.0.11 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.	5.4	More Details
CVE-2026-116312	Inconsistent transition-capture state in PostgreSQL MERGE allows a table data modifier to make an AFTER trigger process the wrong new row, via a partitioned table MERGE that performs an INSERT before an UPDATE. Within major versions 15-18, minor versions before PostgreSQL 18.7, 17.12, 16.16, and 15.20 are affected. Versions before PostgreSQL 15 are unaffected.	5.4	More Details
CVE-	Missing authorization in PostgreSQL DROP OWNED allows a role to remove itself from restrictive row level		

2026-116311	security policies, thereby reading or modifying rows that the policy was intended to deny, via queries after the DROP OWNED. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	5.4	More Details
CVE-2026-110195	IBM ContextForge MCP Gateway 1.0.0 through 1.0.11 could allow an authenticated caller to bypass upstream credential-level authorization policies due to an insufficiently specific cache key in the RFC 8693 token exchange cache, enabling reuse of cached upstream bearer tokens across different credentials belonging to the same user.	5.4	More Details
CVE-2026-126484	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability in printed_fee_sheet.php that allows authenticated portal patients to inject script by setting unescaped appointment comments (pc_hometext). Attackers can submit HTML payloads via the form_comments field in add_edit_event_user.php that execute when staff open the patient's fee sheet, acting within the staff session.	5.4	More Details
CVE-2026-2982	The WP Table Builder – Drag & Drop Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation by lower-privileged users requires an administrator to explicitly allow those roles in plugin settings. While it is possible to assign subscriber-level roles with the ability to create tables, such privileges are usually assigned to the more appropriate contributor, author, or editor level roles.	5.4	More Details
CVE-2026-126462	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability that allows authenticated users with Eye Exam edit permission to inject scripts via the Next Visit Orders PLAN[] field. Attackers can store a payload closing the textarea in view.php, executing JavaScript when another user opens the Eye Exam editor to steal session identifiers or clinical data.	5.4	More Details
CVE-2026-123765	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache Sling XSS. xssAPI.getStyleToken() accepts markup in unquoted urls. This issue affects Apache Sling XSS: before 2.4.14. Users are recommended to upgrade to version 2.4.14, which fixes the issue.	5.4	More Details
CVE-2026-126493	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability that allows low-privileged patient portal users to inject JavaScript via the tableArgs field of the onsiteportalactivity API. Attackers can store a payload with spaces that breaks out of an unquoted data-delete-id attribute, executing script when providers click the delete button on the audit review page.	5.4	More Details
CVE-2026-126942	Zipline before 4.6.2 contains a missing authorization vulnerability in POST /api/user/folders that allows authenticated users to reparent other users' files by supplying their file IDs. Attackers can harvest file IDs from public folders and create a folder seeded with them, disclosing victims' file URLs and removing those files from their folder views.	5.4	More Details
CVE-2026-92379	An improper neutralization of input during web page generation vulnerability in the Notification API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read or write specific files.	5.4	More Details
CVE-2026-127203	AppFlowy Cloud through 0.9.64 contains a stored cross-site scripting vulnerability that allows authenticated workspace members to upload blobs with unvalidated Content-Type values that are later served inline without a Content-Disposition header or authentication on the retrieval route. Attackers can upload a text/html or image/svg+xml blob via put_blob_handler, which is then rendered as an active same-origin document through the unauthenticated get_blob_handler endpoint and cached immutably for one year, enabling persistent script execution against any visitor who accesses the URL.	5.4	More Details
CVE-2026-126946	Zipline from 4.3.0 before 4.5.0 contains a stored cross-site scripting vulnerability that allows authenticated low-privilege users to inject HTML through unescaped embed settings in SSR meta tags. Attackers can set malicious embedTitle, embedDescription, embedSiteName, or embedColor values via PATCH /api/user to execute JavaScript in browsers of visitors opening their file view pages.	5.4	More Details
CVE-2026-126947	Zipline before 4.5.0 contains a stored open redirect vulnerability that allows authenticated users to set arbitrary short URL destinations by abusing missing scheme validation in POST /api/user/urls. Attackers can store javascript: URIs or attacker-controlled URLs as destinations, causing visitors of the trusted short link to be redirected to phishing or malware pages.	5.4	More Details
CVE-2026-126778	Wallos 4.4.0 before 5.10.3 contains a stored cross-site scripting vulnerability in endpoints/cronjobs/sendnotifications.php that allows registered users to inject scripts via unescaped notification service responses. Attackers can point their Mattermost webhook URL or Web Push endpoint at a controlled server returning JavaScript, which executes in the administrator's session when sendnotifications.php is opened.	5.4	More Details
CVE-2026-126810	WWBN AVideo 29.1.0 through 29.7.1 contains a stored cross-site scripting vulnerability that allows registered users to inject markup through the channel About field rendered in feed/index.php. Attackers can store an unquoted event-handler payload that bypasses feedHtmlDescription() filtering and executes via rss-style.xsl for any visitor, including administrators, viewing the channel feed.	5.4	More Details
CVE-2026-	OpsTree REMS through 1.0.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject scripts by uploading attachments with spoofed text/html Content-Type. Attackers can upload HTML files named like test.html.pdf that render in the REMS origin via Preview, executing JavaScript in victims'	5.4	More Details

126771	browsers.		
CVE-2026-129142	paicoding commit 766c48b through commit 903adce contains a stored cross-site scripting vulnerability in payment notifications, where NotifyMsgListener inserts the payer's display name unescaped and notify-system-item.html renders it via th:utext. Authenticated attackers can set a malicious display name and start a pending payment on a paid article, executing script in the author's browser when the author views notifications.	5.4	More Details
CVE-2026-116425	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains unauthorized access vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering and Unauthorized access.	5.4	More Details
CVE-2026-116424	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains Unauthorized access vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering and Unauthorized access.	5.4	More Details
CVE-2026-116423	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains an Improper Verification of Cryptographic Signature vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges and Information tampering.	5.4	More Details
CVE-2026-108338	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Apache Roller 5.0.1 through 6.1.6 allows an authenticated user with the Author role on a weblog to store script in entry tags submitted through AtomPub. Roller's tag filter allowed HTML characters in tag names, and the bundled gaurav, fauxcoly and frontpage themes and the showEntryTags macro print tag names without escaping, so the script runs in the browser of anyone who views the weblog. This matters when weblog authors are not trusted with script (weblogAdminsUntrusted=true, the default since 6.1.4). AtomPub is disabled by default. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which removes HTML characters from tag names, including names stored earlier.	5.4	More Details
CVE-2026-111824	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Apache Roller 6.1.6 allows an authenticated user with the Author role on a weblog that uses a custom theme to store script that runs in the browser of anyone who opens the file's resource URL. The fix for CVE-2026-82387 serves uploaded media as a download unless it is an image, audio, video, PDF or plain text, but media files found through a custom theme were served with the type their path implies, and the upload form let the uploader choose that path. Media uploads are disabled by default. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which serves these files under the same rules as other media and no longer accepts the path from the upload form.	5.4	More Details
CVE-2026-118413	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Apache Roller 4.0 through 6.1.6 allows a weblog administrator to store script that runs in the browsers of the weblog's visitors. Blogroll links imported from an OPML file were not checked, and the default theme printed them without escaping. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which accepts only web links on import and escapes them on output.	5.4	More Details
CVE-2026-118414	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Apache Roller 6.1.2 through 6.1.6 allows a weblog administrator to store script that runs in the browsers of the weblog's members when they open their main menu. The HTML-stripping routine kept a tag that was not closed, and the main menu printed the weblog description without escaping. Users are recommended to upgrade to Apache Roller 6.1.7 or later.	5.4	More Details
CVE-2026-129133	MRBS before 1.13.0 contains a CSV formula injection vulnerability that allows authenticated users to inject spreadsheet formulas because the escape() function in web/report.php fails to neutralize leading formula characters. Attackers can store formulas in booking names, descriptions or custom fields that execute when privileged users open exported CSV reports, enabling data exfiltration or command execution via DDE.	5.4	More Details
CVE-2026-128970	Psono Server Community Edition versions 1.12.6 through 7.5.0 and Psono Server Enterprise Edition before 7.5.1 do not require accepted group membership when authorizing deletion of group share-rights. The DELETE /share/right/ endpoint checks for a membership matching the target group, the authenticated user, and share_admin=True, but omits accepted=True. An authenticated remote attacker who has been invited to a group with share-admin privileges, and who knows a group share-right UUID, can therefore delete that group's share-right record without accepting the invitation or after declining it. Pending invitations have accepted=None, while declined invitations retain accepted=False and the share_admin flag. Deletion revokes the group's access to the affected share and its contained secrets for all accepted group members, without deleting the underlying data or disclosing secret contents. The issue was fixed in version 7.5.1 of both editions, released on 2026-10-13.	5.4	More Details
CVE-2026-124263	Cross-Site Request Forgery (CSRF) vulnerability in plainware Locatoraid Store Locator locatoraid allows Cross Site Request Forgery.This issue affects Locatoraid Store Locator: from n/a through 3.9.75.	5.4	More Details
CVE-2026-126658	ByteStash 1.5.10 before 1.6.2 contains an insufficient session expiration vulnerability that allows holders of API keys to keep access after account deactivation because validateApiKey never checks account status. Attackers holding a deactivated account's API key can read, create, modify and delete its snippets via /api/snippets and use every MCP tool via /mcp.	5.4	More Details
CVE-2026-	A Cross-Site Scripting via Unencoded Font Metadata in Apache Batik SVGFont. This issue affects Apache XML	5.4	More

40853	Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.		Details
CVE-2026-129140	paicoding 1.0.0 through 1.0.3 contains a stored cross-site scripting vulnerability in image upload because ImageServiceImpl.validateStaticImg accepts SVG files, which are then served from the site origin when local storage is used. Authenticated attackers can upload script-bearing SVG images that execute when victims view them, stealing the non-HttpOnly f-session cookie to hijack accounts.	5.4	More Details
CVE-2026-129141	paicoding 1.0.0 through 1.0.3 contains a stored cross-site scripting vulnerability because SeoInjectService embeds user profile text without escaping in an inline JSON-LD script element. Authenticated attackers can add a closing script tag followed by HTML to their profile, executing scripts for visitors of their profile page and stealing the non-HttpOnly f-session cookie.	5.4	More Details
CVE-2026-129341	The web endpoint that removes an attachment skipped the permission check when the request came from the user who had uploaded the attachment, and it was reachable with read access to issues or pull requests. A user who had uploaded a release asset could still delete it after losing write access to the repository. The endpoint now only deletes attachments that the user uploaded and that are not yet linked to an issue, comment or release.	5.4	More Details
CVE-2026-129156	DjangoBlog commit d186b1c through commit 6134ed6 contains a stored cross-site scripting vulnerability that allows authenticated OAuth users to inject script via an unescaped nickname in comment reactions. Attackers can set their OAuth display name to a payload closing the single-quoted data-reactions attribute, then react to a comment to execute script in article visitors' browsers.	5.4	More Details
CVE-2026-126365	Astro is a web framework for content-driven websites. Prior to @astrojs/prism 4.1.2, and from @astrojs/markdoc 0.3.0 until 2.1.2, runHighlighterWithAstro() returned code unchanged when Prism had no grammar for the requested language, and callers inserted that result as raw HTML. A code block labeled with an unsupported language could therefore render embedded HTML and script instead of displaying it as text. The Prism component was affected when applications supplied untrusted code with an unsupported or attacker-controlled lang, and the @astrojs/markdoc prism() extension was affected for less-trusted content authors even when Markdoc's ordinary HTML rendering was disabled. This issue is fixed in @astrojs/prism 4.1.2 and @astrojs/markdoc 2.1.2.	5.4	More Details
CVE-2026-124686	In Progress® Kendo® UI for jQuery versions prior to 2026.4.1111, kendo.init() compiles data-* attribute values with new Function when an invalid JSON object is supplied. An attacker with low privileges who can control these attribute values can inject JavaScript that executes during declarative widget initialization when a user loads or interacts with an affected page. Successful exploitation can compromise the confidentiality and integrity of data accessible in the user's browser context. The issue was reported in version 2022.3.1109; the first affected release has not been established.	5.4	More Details
CVE-2026-129158	ragent 1.1.0 contains a stored cross-site scripting vulnerability that allows authenticated users to inject scripts by uploading SVG knowledge-base documents served inline as image/svg+xml. Attackers can upload a script-bearing SVG via /knowledge-base/{kb-id}/docs/upload so that victims opening /knowledge-base/docs/{docId}/file execute it in the application origin, enabling account takeover.	5.4	More Details
CVE-2026-126411	Frappe HRMS 16.0.0 before 16.50.0 lacks authorization checks on certain HR workflow endpoints, letting authenticated users access records they are not permitted to view. Any logged-in user, including one with only the Employee role, can read candidate record details and employee email addresses, and cause emails to be sent to employees.	5.4	More Details
CVE-2026-129144	paicoding 1.0.3 contains a payment bypass vulnerability that allows authenticated attackers to unlock paid articles by guessing weak payment confirmation codes. Attackers can start a payment, enumerate roughly 2000 IdUtil.genPayCode counter values, and submit the matching verifyCode to the unauthenticated callback to mark it paid.	5.4	More Details
CVE-2026-126419	OpenEMR before 8.5.0 contains a missing authorization vulnerability in the esign_form_submit handler of library/ESign/Form/Controller.php that verifies only the caller's password, not access to the patient, encounter, or form type. Authenticated core users can supply arbitrary formId, formDir, and encounterId values to sign and lock any patient's clinical form, creating unauthorized approval records and blocking normal editing.	5.4	More Details
CVE-2026-128022	FrankenPHP before 1.13.2 contains a resource exhaustion vulnerability that allows unauthenticated clients to tie up PHP threads because queued requests are not cancelled when clients disconnect. Attackers can send many requests and close connections immediately, forcing handleRequestWithRegularPHPThreads and worker handlers to execute them and delay all clients sharing the thread pool.	5.3	More Details
CVE-2026-126939	Zipline before 4.6.4 contains an information disclosure vulnerability in GET /api/server/folder/:id that allows unauthenticated attackers to list files in non-public upload-only folders. Attackers who know the folder UUID can supply the page query parameter to bypass the metadata-only early return and enumerate file names, IDs, MIME types, sizes, and view counts.	5.3	More Details
CVE-2026-128045	OpenMage Magento-LTS before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains an authorization bypass in the /rss/order/status feed because its URL key is unsigned Base64-encoded JSON of the order, increment, and customer ids. Unauthenticated attackers can forge keys from enumerated sequential ids to read other customers' names, items, prices, totals, and status comments when order-status RSS is enabled.	5.3	More Details

CVE-2026-125802	Insertion of Sensitive Information Into Sent Data vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Retrieve Embedded Sensitive Data.This issue affects Spectra: from n/a through 2.20.5.	5.3	More Details
CVE-2026-105880	Authorization Bypass Through User-Controlled Key vulnerability in Tobias WebinarIgnition webinar-ignition allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebinarIgnition: from n/a through 4.27.125.	5.3	More Details
CVE-2026-107525	Dell PowerStore contains an information disclosure vulnerability. An unauthenticated attacker could exploit this vulnerability to obtain service metadata useful for further attacks.	5.3	More Details
CVE-2026-126387	n8n before 2.46.1 contains an arbitrary file read vulnerability that allows authenticated members to read server files by supplying absolute paths to the Browser Use browser_upload tool. Attackers with a connected remote browser session can have Playwright read files such as instance configuration from the n8n server and retrieve their contents from the page.	5.3	More Details
CVE-2026-126417	OpenEMR before 8.5.0 contains an access control flaw in get_claim_file.php: with location=tmp, it serves any file in the shared temporary directory without verifying the file is a claim for the caller. Users with acct/eob or acct/bill write access can request key=ccda.xml to download the most recently validated patient's complete C-CDA clinical document.	5.3	More Details
CVE-2026-126394	vLLM 0.30.0 before 0.31.0 contains a resource exhaustion vulnerability in OpenCVDynamicOpenPanguVideoBackend, which uses request-controlled num_frames without an effective ceiling. Unauthenticated attackers can send /v1/chat/completions or /tokenize requests selecting the openpangu video_backend with a huge num_frames, forcing np.linspace allocations and CPU work that OOM-kill the API server.	5.3	More Details
CVE-2026-125808	Missing Authorization vulnerability in HTMega HT Mega ht-mega-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HT Mega: from n/a through 3.2.8.	5.3	More Details
CVE-2026-128237	Scapy before 2.8.0 contains a denial of service vulnerability in BER_num_dec() and BERcodec_OID.do_dec() that allows remote attackers to exhaust CPU by supplying oversized OID arcs. Attackers can send ASN.1/BER data with many base-128 continuation bytes to cause quadratic CPU consumption or an uncaught ValueError crash on Python 3.11+.	5.3	More Details
CVE-2026-125819	Missing Authorization vulnerability in PublishPress Gutenberg Blocks advanced-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gutenberg Blocks: from n/a through 3.7.6.	5.3	More Details
CVE-2026-125821	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in PT Norther Lights Production MapSVG mapsvg-lite-interactive-vector-maps allows Code Injection.This issue affects MapSVG: from n/a through 9.0.4.	5.3	More Details
CVE-2026-128238	Scapy before 2.8.0 contains an uncontrolled recursion vulnerability in the BER/ASN.1 decoder in scapy/asn1/ber.py that allows unauthenticated remote attackers to crash parsing applications. Attackers can send a single 833-byte packet with 250 nested ASN.1 SEQUENCE structures to trigger an unhandled RecursionError, terminating TLS, SNMP, X.509, or LDAP parsers even with safe=True.	5.3	More Details
CVE-2026-121771	Insertion of Sensitive Information Into Sent Data vulnerability in PublishPress Gutenberg Blocks advanced-gutenberg allows Retrieve Embedded Sensitive Data.This issue affects Gutenberg Blocks: from n/a through 3.7.6.	5.3	More Details
CVE-2026-125814	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Rymera Web Co Product Feed PRO for WooCommerce woo-product-feed-pro allows Code Injection.This issue affects Product Feed PRO for WooCommerce: from n/a through 13.5.8.	5.3	More Details
CVE-2026-125792	Missing Authorization vulnerability in Andy Moyle Church Admin church-admin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Church Admin: from n/a through 5.1.8.	5.3	More Details
CVE-2026-128331	Miniflux before 2.3.5 contains an unverified password change vulnerability that allows holders of a signed-in session to change the account password without supplying the current password. Attackers with a stolen session cookie or unattended device can submit new password fields via updateSettings to lock out the owner and take over the account.	5.3	More Details
CVE-2026-126447	OpenEMR before 8.5.0 contains a missing authorization vulnerability in trusted-messages-ajax.php that allows any authenticated core user to send Direct messages without the patients/notes permission. Attackers with zero-ACL accounts can submit chosen recipients and message bodies sent via the clinic's phiMail credentials, impersonating the clinic to deliver fraudulent clinical communications.	5.3	More Details
CVE-2026-	Missing Authorization vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spectra: from n/a through 2.20.5.	5.3	More Details

128834			
CVE-2026-126441	OpenEMR before 8.5.0 contains an insecure direct object reference vulnerability in the CAMOS rx_print.php printer that allows authenticated users to read other patients' prescriptions. Attackers can submit forged chrx_ parameters with global prescription IDs to disclose drug names, dosages, directions, and refill counts without medication permissions.	5.3	More Details
CVE-2026-126439	OpenEMR before 8.5.0 contains a missing authorization vulnerability in ccdaservice/ccda_gateway.php that fails to enforce the patients/pat_rep permission, accepting any authenticated core session. Authenticated users without patient-report permission can request the report_ccd_view action to retrieve the selected patient's C-CDA clinical summary, including diagnoses, medications, laboratory results, and identifiers.	5.3	More Details
CVE-2026-128991	xschem 2.9.9 through 3.4.7 contains an out-of-bounds read vulnerability in read_xschem_file() in src/save.c that mishandles embedded-symbol records lacking a preceding instance. Attackers can supply a crafted schematic beginning with a "[" record, causing xschem to read and dereference memory below the instance array and crash.	5.3	More Details
CVE-2026-124409	Missing Authorization vulnerability in VillaTheme CURCY woo-multi-currency allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CURCY: from n/a through 2.2.21.	5.3	More Details
CVE-2026-126955	Glance from 0.8.0 before 0.8.8 contains an observable response discrepancy in handlePageRequest and handlePageContentRequest that allows unauthenticated attackers to enumerate configured page slugs. Attackers can request candidate names against /{page} or /api/pages/{page}/content/ and compare 303/401 versus 404 status codes to discover hidden page names.	5.3	More Details
CVE-2026-128345	ExcelJS through 4.4.0 contains a regular expression denial of service vulnerability in slideFormula in lib/utils/shared-formula.js when translating shared formulas to child cells. Attackers can supply a crafted spreadsheet with very long master formulas, such as runs of hyphens, causing quadratic regex backtracking that blocks the Node.js event loop.	5.3	More Details
CVE-2026-126396	vLLM from 0.24.0 before 0.31.0 contains a resource exhaustion vulnerability in the MiniMax M3 VL video processor, which accepts request-level min_pixels without range or min_pixels <= max_pixels validation. Its video-wide pixel budget is enforced only when max_long_side_pixel is set, and that value defaults to None. API clients can supply a large min_pixels via mm_processor_kwargs to enlarge every decoded frame, causing excessive CPU and host-memory consumption that may disrupt workers or the service.	5.3	More Details
CVE-2026-125815	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Noah Hearle We’re Open! opening-hours allows Code Injection.This issue affects We’re Open!: from n/a through 2.8.	5.3	More Details
CVE-2026-126395	vLLM from 0.14.0rc1 before 0.31.0 contains an information disclosure vulnerability in sanitize_message() whose lowercase-only regex fails to scrub uppercase PIL image addresses. Unauthenticated attackers can send a crafted PNG to endpoints such as /tokenize, triggering HF-processor errors that leak live server heap addresses useful for ASLR bypass.	5.3	More Details
CVE-2026-112830	Missing Authorization vulnerability in Brizy Brizy brizy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Brizy: from n/a through 2.8.25.	5.3	More Details
CVE-2026-125432	Weak Password Recovery Mechanism for Forgotten Password vulnerability in RelyWP reCAPTCHA for WooCommerce recaptcha-woo allows Password Recovery Exploitation.This issue affects reCAPTCHA for WooCommerce: from n/a through 1.4.7.	5.3	More Details
CVE-2026-125440	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Cristián Lávaque s2Member s2member allows Code Injection.This issue affects s2Member: from n/a through 261106.	5.3	More Details
CVE-2026-124414	Weak Authentication vulnerability in VideoWhisper.com Broadcast Live Video videowhisper-live-streaming-integration allows Authentication Abuse.This issue affects Broadcast Live Video: from n/a through 7.3.15.	5.3	More Details
CVE-2026-126993	A security flaw has been discovered in SiteServer SSCMS up to 7.2.2. Impacted is an unknown function of the file /api/v1/captcha. Performing a manipulation of the argument Value results in inadequate encryption strength. 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.	5.3	More Details
CVE-2026-125825	Missing Authorization vulnerability in Webful Creations RepairBuddy computer-repair-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RepairBuddy: from n/a through 4.1236.	5.3	More Details
CVE-2026-121014	Missing Authorization vulnerability in Ahmad WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through 2.7.2.	5.3	More Details

CVE-2026-126615	The sign-in of Progressive Robot hMailServer 6.2.22-pre2 through 6.3.7 takes for an account names that are not its address but under which the database's own comparison finds it, while the per-name lockout and the compromised-account hold are kept by the name as the client gave it. This allows a remote unauthenticated attacker to go on guessing an account's password beyond the lockout's threshold, and anyone who has the password of an account held for review to sign in to it. The per-name lockout (from 6.2.22-pre2; AccountLockoutThreshold in hMailServer.ini, 0, off, by default) locks a name after repeated failed sign-ins. The hold (from 6.3.4, where the compromised-account detection is set to enforce, which is not the default) refuses an account judged to have been taken over. Both are asked, before the password, of the name the client gave: trimmed, in lower case and with a domain alias or the default domain applied. The account whose password the sign-in then checks is whichever one the database finds under that name. The databases find an account under spellings that this key counts apart. MySQL and MariaDB find it under one with accented letters in place of plain ones, and MariaDB 11.8, in a database made before 6.3.4, also under one with full-width letters, with a single letter in place of a pair of plain ones, or with characters its comparison ignores in any number. SQL Server and SQL Server Compact find it under one with full-width letters or with characters their comparison ignores in any number, and SQL Server also under one with a single letter in place of a pair of plain ones, with a character of Latin-1 in place of a digit and, for an address holding letters of Latin-1 outside ASCII, under those letters in the other case, and, under an accent-insensitive collation, with accented letters. PostgreSQL finds it under one holding a letter whose lower case under the database's locale is a plain letter, and, for an address holding letters outside ASCII, under those letters in the other case; on the build for musl (from 6.3.6) the server's own lower case folds nearly all of these too. On every database, a domain alias saved with white space at the end of its name gives such a spelling too, and on every database but PostgreSQL so does an account's bare local part where the default domain was saved with spaces at its end and no other white space (neither is the default). Each such spelling has a lockout threshold of its own, so the lockout limits the guesses at an account only to its threshold times the number of the account's spellings. That is far beyond any threshold for most addresses on MySQL and MariaDB, and without limit on SQL Server, on SQL Server Compact, the database the Windows installer uses by default, and before 6.3.4 on MariaDB 11.8. A locked name is got round under another spelling. A held account is signed in to under another spelling with its password over IMAP, POP3 and SMTP AUTH, and, where they are turned on (off by default), over ManageSieve, the REST API and the webmail. IMAP LOGIN, offered as installed, carries such spellings on MySQL, MariaDB and SQL Server Compact, and, on SQL Server and PostgreSQL, for some addresses; the sign-ins that carry a name as UTF-8 carry them for the others on SQL Server, and on PostgreSQL for those holding one of the plain letters another letter lowers to or a letter outside ASCII with another case. The same lookup mapped to accounts the names given by an OAuth 2.0 token, a client certificate, a Kerberos ticket and an OpenID Connect or SAML identity provider, where those are set up (none is by default), so that a name an issuer gave to one party could sign in to another's account; OAuth 2.0 tokens were mapped so from 6.2.0, before the per-name lockout existed. A name holding a NUL character, carried from 6.3.0 on Linux and 6.3.3 on Windows, failed the statement on MySQL, MariaDB and PostgreSQL.	5.3	More Details
CVE-2026-126616	The auto-ban of Progressive Robot hMailServer 6.2.0 through 6.3.3, with a MySQL or MariaDB database, can be kept from banning an address after repeated failed logons, which allows a remote unauthenticated attacker to go on guessing account passwords from a single address without being banned. The server makes its MySQL tables in MySQL's utf8 character set, which holds no character outside the Basic Multilingual Plane, sends its statements as UTF-8 over a utf8mb4 connection and leaves the database's default strict mode in place. From 6.2.0 it decodes the user name of a SASL PLAIN logon as UTF-8, so the name can hold such a character. When the failed logons counted from one address reach MaxInvalidLogonAttempts (3 by default), the server clears that address's count, saves an IP range named "Auto-ban: " followed by the user name of the logon that reached the limit, and drops the connection. If such a character is in the part of the user name that the range's name keeps (the name is cut to 100 characters), the database refuses the range: no range is saved, the address is not refused, and, its count having already been cleared, it is given the next full set of attempts. An attacker can in this way spend all but the last attempt of each set on password guesses, and make the last under such a name. On Windows, POP3 AUTH PLAIN reaches it on a server as installed, and IMAP AUTHENTICATE PLAIN where IMAP SASL authentication is turned on (off by default); on Windows and on Linux (from 6.3.0), SMTP AUTH PLAIN reaches it where plain-text authentication is allowed (off by default), and ManageSieve and CardDAV where they are turned on (off by default). Each failed save is reported in the server's error log. A database whose strict mode has been turned off stores the character as a question mark and makes the first such ban, but refuses every later ban named after the same user name, or after one holding other such characters in their place, as a duplicate while the first stands, since the server cannot look up a name holding such a character there.	5.3	More Details
CVE-	The auto-ban of Progressive Robot hMailServer 6.0.0-B1 through 6.3.7 can be kept from banning an address after repeated failed logons, which allows a remote unauthenticated attacker who can connect from two or more addresses to go on guessing account passwords - over SMTP AUTH, IMAP and POP3, and over ManageSieve, CalDAV/CardDAV and the REST API where those are turned on (off by default) - without being banned. When the failed logons counted from one address reach MaxInvalidLogonAttempts (3 by default), the server clears that address's count, saves an IP range that refuses the address for AutoBanMinutes (60 by default) and drops the connection. The range is named "Auto-ban: " followed by the user name of the logon that reached the limit, and no two ranges may have the same name. The server chooses the name by checking candidates as written - the name, then the name with a number, a random suffix or a GUID added - and only then cuts it to the 100 characters the database column holds, so that with a user name of 90 characters or more every candidate is the same once cut. While one range named after such a user name stands, every later ban named after a user name with the same first 90 characters therefore fails at the database: no range is saved, the address is not refused, and, its count having already been cleared, it is given the next full set of attempts. A user name of 78 to 89 characters makes later bans fail in the same way: from the second, the third or the twelfth on, depending on its length and the database, or, from 78 to 85 characters, by chance. An attacker who has once had an address		

2026-126618	banned under such a name can in this way keep guessing passwords from any other address, ending each set of attempts with a logon under a name of that kind; each failed save is reported in the server's error log (as the database error HM5032, and from 6.2.19 also as HM6099). On SQL Server a user name holding characters outside the database's code page has the same effect at any length, because the check compared names in that code page; that save is refused by the server's own check of the name, with no database error, and is reported only from 6.2.19 (HM6099). A user name holding a NUL character, which the web services listener's HTTP Basic sign-in (off by default) carries from 6.3.3 and, on the Linux builds, IMAP LOGIN, offered as installed, from 6.3.0, makes bans fail at any length: on MySQL, MariaDB and PostgreSQL the statements that check the name and save the range end at the character, so that every ban named after such a name fails, from the first and from a single address, and, its count having already been cleared, the address is given the next full set of attempts; on SQL Server and SQL Server Compact the name is bound only as far as the character, so that while one range under the part before it stands, every later ban named after such a name fails. On SQL Server, and on MySQL and MariaDB for an account whose local part has nine characters or more, a guess at the account can itself carry a name of that kind, since those databases find an account under its address followed by spaces (and SQL Server also under one holding characters its comparison ignores), so that not even a MaxInvalidLogonAttempts of 1, which bans each failed logon under the name it gave, avoids it there.	5.3	More Details
CVE-2026-125827	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 5.31.0.	5.3	More Details
CVE-2026-126626	The web services listener of Progressive Robot hMailServer 6.3.3 through 6.3.7 counts every failed CardDAV, CalDAV or Autodiscover sign-in from a proxy it trusts - one on the same machine, or one named in WebServicesTrustedProxies, whose X-Forwarded-Proto it believes - against the proxy's own address, which allows a remote unauthenticated attacker who can reach the proxy to have that address banned from the server's mail listeners. The listener, off by default (WebServicesHttpPort and WebServicesHttpsPort 0), signs an account in with HTTP Basic over HTTPS for CardDAV from 6.3.3 and for CalDAV and Outlook Autodiscover from 6.3.4. Behind a TLS-terminating proxy, which the server trusts when it is on the same machine or named in WebServicesTrustedProxies, the listener takes the client's HTTPS from the proxy's X-Forwarded-Proto header, but it does not believe X-Forwarded-For and sees the proxy's address for every client. Each failed sign-in counted towards the auto-ban against that address, so that failed sign-ins through the proxy from anybody, under any user name, reaching MaxInvalidLogonAttempts (3 within 30 minutes by default) wrote an IP range that refused the proxy's address at the SMTP, POP3, IMAP and ManageSieve listeners for AutoBanMinutes (60 by default), and could write it again each time it lapsed. For a proxy on the same machine that address is the loopback address, so that a webmail on that machine, local scripts that submit mail and the other local clients of the mail listeners were shut out; for a proxy at another address that also carries mail, every mail client behind it was. Such a proxy forwarding to the listener's HTTPS port, re-encrypting, was counted against in the same way, and listing it in WebServicesTrustedProxies did not spare it. The auto-ban is on by default and AutoBanNeverBan, which spares an address, is empty by default; the listener itself went on serving the proxy.	5.3	More Details
CVE-2026-115600	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 2.8.3.	5.3	More Details
CVE-2026-115501	IBM i 7.3 7.4, 7.5, and 7.6 is vulnerable to a stack buffer overflow, caused by improper bounds checking in the QFileSvr.400 file system. By sending a command in the QFileSvr.400 file system, a local authenticated attacker could cause undefined behavior.	5.3	More Details
CVE-2026-9821	IBM Cyber Fraud 1.0.0 through 1.1.0 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written to log files.	5.3	More Details
CVE-2026-106027	The Oxygen MyData for WooCommerce WordPress plugin before 3.0.9 does not have proper authorisation, nor validate the authenticity of the request, on one of its payment callbacks, allowing unauthenticated users to mark arbitrary WooCommerce orders as completed.	5.3	More Details
CVE-2026-129173	A security flaw has been discovered in Stirling-Tools Stirling-PDF up to 3.3.0. Affected is the function WorkflowParticipantController.getParticipantDetails of the file app/proprietary/src/main/java/stirling/software/proprietary/workflow/controller/WorkflowParticipantController.java of the component Participant Details Endpoint. Performing a manipulation results in insufficient session timeout value. Remote exploitation of the attack is possible. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-124817	The Clockinator Lite WordPress plugin before 1.1.0 does not check authorisation or ownership when updating leave requests, allowing unauthenticated users to modify any leave record, including approving or rejecting requests and reassigning them to other users.	5.3	More Details
CVE-2026-124665	The Order Tracking WordPress plugin before 3.6.2 does not verify that a visitor owns the customer or sales representative account whose orders they request, and the account numbers default to sequential values, allowing unauthenticated users to retrieve the order history of every customer and sales representative, including order contact email addresses in some versions.	5.3	More Details
CVE-	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WP Chill Strong		

2026-121028	Testimonials strong-testimonials allows Code Injection.This issue affects Strong Testimonials: from n/a through 3.3.17.	5.3	More Details
CVE-2026-124648	The TI WooCommerce Wishlist WordPress plugin before 2.13.0 does not verify that a visitor who is not logged in owns a registered user's wishlist before letting them manage it, allowing unauthenticated users who know or guess a wishlist's share key to delete items from other customers' wishlists.	5.3	More Details
CVE-2026-119039	The Defender Security WordPress plugin before 6.4.1 does not verify that the client IP address it derives for its firewall and lockout decisions actually originates from a trusted source, trusting a user-supplied value by default, allowing unauthenticated attackers to spoof their IP address and evade IP-based protections such as login lockout and IP banning, impersonate an allowlisted address, and poison the Defender Security WordPress plugin before 6.4.1's activity logs.	5.3	More Details
CVE-2026-105984	The Email Marketing 4Dem WordPress plugin through 2.0.5 does not perform authorization or capability checks on several of its AJAX actions, allowing unauthenticated users to destroy its stored configuration and delete its records.	5.3	More Details
CVE-2026-116322	Improper locking in PostgreSQL startup processing allows an unauthenticated network client to trigger a server restart, via arranging for authentication_timeout to arrive while it holds a spinlock during cancel handling. Within major version 18, minor versions before PostgreSQL 18.7 are affected. Versions before PostgreSQL 18 are unaffected.	5.3	More Details
CVE-2026-126614	The web services listener of Progressive Robot hMailServer 6.3.3 through 6.3.7 does not apply the server's IP ranges to the connections it accepts, which allows a remote unauthenticated attacker to go on guessing account passwords at the listener's sign-ins after the auto-ban has banned the attacker's address. The listener is off by default (WebServicesHttpPort and WebServicesHttpsPort 0). From 6.3.3 its CardDAV, and from 6.3.4 its CalDAV and its Outlook Autodiscover answer to a request that carries credentials, sign an account in with HTTP Basic over HTTPS. A failed sign-in there counts towards the auto-ban as a failed logon on any other protocol does: when the failures counted from one address reach MaxInvalidLogonAttempts (3 within 30 minutes by default), the server writes an IP range that refuses the address for AutoBanMinutes (60 by default), and the SMTP, POP3, IMAP and ManageSieve listeners refuse it. The web services listener asked no IP range when it accepted a connection (in 6.3.3 nothing, from 6.3.4 the country policy alone), so it went on serving such an address, whether its ban had been earned there or on another protocol, and also an address that an administrator's IP range allowing nothing holds. Each failed sign-in there closed only its own connection, and the next connection was accepted, during the ban and after it. The firewall rule and command the auto-ban can drive (AutoBanFirewall and AutoBanCommand, off by default) are told only the SMTP, POP3 and IMAP ports, so that the firewall rule and the packaged hook did not close the listener's ports, and the fail2ban jail packaged for Linux (off by default) lists only the mail and ManageSieve ports. The only limit left on the guesses at one account there was the per-name lockout (AccountLockoutThreshold in hMailServer.ini, 0, off, by default), which has a separate defect fixed in the same release. The flaw is reached on the listener's HTTPS port: behind a TLS-terminating proxy the listener sees the proxy's address for every client, and a ban never named the client there.	5.3	More Details
CVE-2026-92408	The WPS Bookings for WooCommerce WordPress plugin before 3.13.1 does not validate a price value taken from user input before using it to set the product price, allowing unauthenticated users to purchase bookable services at a price of their choosing, including zero.	5.3	More Details
CVE-2026-123668	The GetPaid WordPress plugin from 2.8.63 to 2.8.64 does not ensure item quantities on its payment forms are whole numbers, allowing unauthenticated users to have an invoice for a priced item marked as paid without being charged.	5.3	More Details
CVE-2026-123703	The Security For WooCommerce WordPress plugin through 1.0.16 does not check that the requester is authorised before ending a user's login sessions, allowing unauthenticated visitors to log out any user, including administrators, and to keep them logged out by repeating the request.	5.3	More Details
CVE-2026-127119	Unverified ownership of the default cluster log location in the EMR module in AWS SDK for pandas (awswrangler) from 1.1.0 before 3.18.0 might allow remote actors to read Amazon EMR cluster logs, including job step output, via a pre-created S3 bucket. To remediate this issue, users should upgrade to version 3.18.0 or later. Users who can't upgrade immediately should pass an explicit log location, or create the default EMR log bucket in their own account in each region they use.	5.3	More Details
CVE-2026-128085	OpenTelemetry-Go is the Go implementation of OpenTelemetry. From SDK version 1.33.0, SDK log version 0.9.0, and trace version 1.35.0 until version 1.47.0, the AttributeValueLengthLimit and WithAttributeValueLengthLimit truncation paths in sdk/internal/attrnorm, sdk/log/internal/attrnorm, and trace/auto.go do not count valid U+FFFD replacement characters. This is a distinct incomplete-fix defect in the replacement truncation code introduced by the remediation for CVE-2026-81869. Values composed of or dominated by those characters can therefore exceed the configured character and memory bound in span, log-record, and auto-instrumentation trace attributes. Attacker-controlled telemetry attributes can increase retained memory and pipeline pressure, while confidentiality and integrity are not affected. This issue is fixed in version 1.47.0.	5.3	More Details
CVE-2026-	OpenTelemetry-Go is the Go implementation of OpenTelemetry. From version 1.0.0-RC1 until version 1.47.0, baggage.Parse and propagation.Baggage.Extract eagerly materialize every W3C baggage property through parseMember, grow property slices, serialize members, and copy properties into internal/baggage.Item. A valid densely populated baggage header can therefore cause allocation traffic and retained memory disproportionate	5.3	More

128086	to its bounded input size. Remote impact requires baggage extraction to be enabled, attacker-controlled input to reach it, and extraction to run before authentication or on a public route; the evidence establishes increased allocation and garbage-collection pressure but not reliable process termination. This issue is fixed in version 1.47.0.		Details
CVE-2026-123704	The Security For WooCommerce WordPress plugin through 1.0.16 does not restrict access to one of its REST API routes, allowing unauthenticated users to retrieve the email address of every administrator on the site.	5.3	More Details
CVE-2026-64675	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5 and 1.5.1, a single unauthenticated BACnet/IP UDP datagram (port 47808) triggers an out-of-bounds read in xy_color_decode() (src/bacnet/lighting.c), reachable pre-authentication through two default-registered service handlers: the UnconfirmedRequest WriteGroup service (0x0A) and Confirmed WriteProperty on a BACnetXYColor-typed property. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	5.3	More Details
CVE-2026-71363	A flaw was found in AWX. The debug API endpoints (/api/debug/task_manager/, /api/debug/dependency_manager/, /api/debug/workflow_manager/) are registered unconditionally in the URL configuration and use AllowAny permission class with _ignore_model_permissions=True. This allows an unauthenticated remote attacker to repeatedly invoke scheduler operations that acquire database advisory locks and open transactions, potentially leading to resource exhaustion and degraded service availability.	5.3	More Details
CVE-2026-128116	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to versions 2.70.4 and 3.1.1, apps configured with router.resolution: 'server' could treat a pathname beginning with // as a protocol-relative module specifier during client-side navigation. A socially engineered link could therefore make server-side route resolution import and execute JavaScript from another origin in the user's browser. This issue is fixed in 2.70.4 and 3.1.1.	5.3	More Details
CVE-2026-127202	MLflow before 3.18.0 using the FileStore backend contains a path traversal vulnerability that allows unauthenticated remote attackers to write files outside the intended run directory by supplying a malicious model_id parameter to the log outputs API. Attackers can exploit the unvalidated model_id containing ../ sequences via the POST /api/3.0/mlflow/runs/outputs endpoint to create directories and write a meta.yaml file at arbitrary filesystem locations, limited only by the server account's permissions. FileStore was the default backend before 3.7.0 and is opt-in afterward through MLFLOW_ALLOW_FILE_STORE.	5.3	More Details
CVE-2026-126193	Soup Sieve is a CSS selector library for Beautiful Soup. From 0.4 until 3.0, deeply nested CSS pseudo-class selectors can cause recursive parsing to exceed Python’s recursion limit and raise RecursionError . Applications accepting untrusted selectors may experience failure of the affected request or task if the exception is not handled. The demonstrated behavior is recoverable and does not establish an interpreter crash or persistent service-wide denial of service. This vulnerability is fixed in version 3.0.	5.3	More Details
CVE-2026-126189	Soup Sieve is a CSS selector library designed to be used with Beautiful Soup 4. Prior to 4.0.1, Soup Sieve repeatedly searches descendant subtrees for each candidate evaluated by :has() and repeatedly reevaluates a parent containing :has(> ...) for each child, causing quadratic matching on deeply nested or wide attacker-influenced HTML or XML. Applications using ordinary fixed selectors through select(), select_one(), or Beautiful Soup CSS APIs against untrusted documents can have a worker occupied for seconds or minutes, while applications that process only trusted documents are not affected. Selectors compiled with NOCACHE continue to use the old uncached behavior. This issue is fixed in version 4.0.1.	5.3	More Details
CVE-2026-123705	The Security For WooCommerce WordPress plugin through 1.0.16 does not restrict access to one of its REST API routes, allowing unauthenticated users to retrieve a detailed report of the server, PHP and WordPress configuration, including installed Security For WooCommerce WordPress plugin through 1.0.16 and versions and the site administrator's email address.	5.3	More Details
CVE-2026-88813	The YITH WooCommerce Gift Cards WordPress plugin through 4.39.0 does not reconcile the value of a gift card it issues against the amount actually paid for it, instead crediting the new card with the item's pre-discount price, which allows customers to apply an ordinary store coupon at checkout and receive a gift card worth more than they paid.	5.3	More Details
CVE-2026-119171	The Advanced Product Fields (Product Addons) for WooCommerce WordPress plugin from 1.6.22 to 1.7.3 does not validate that a submitted value for a required paid product option matches one of the configured choices, only that it is not empty, allowing unauthenticated users to add a product to the cart and complete an order while skipping the required option's surcharge and paying only the base product price.	5.3	More Details
CVE-2026-123659	The ProfilePress WordPress plugin before 4.17.6 does not restrict the role and user meta filters its member directories accept to those configured by the administrator, allowing unauthenticated users to list accounts a directory was set to hide and to recover user meta values of listed users.	5.3	More Details
CVE-2026-121574	Missing Authorization vulnerability in WP Chill Passster content-protector allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Passster: from n/a through 4.3.20.	5.3	More Details
CVE-2026-124255	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Franky Events Made Easy events-made-easy allows Code Injection.This issue affects Events Made Easy: from n/a through 3.3.5.	5.3	More Details

CVE-2026-123701	The Security For WooCommerce WordPress plugin through 1.0.16 does not have proper authorization checks when resetting its settings, allowing unauthenticated users to reset any section of its configuration to the defaults and so disable security features such as a custom login URL, two-factor authentication, reCAPTCHA, password policies and the firewall.	5.3	More Details
CVE-2026-110989	The RegistrationMagic WordPress plugin before 6.1.0.4 does not verify ownership of the submitted email address before updating the associated WordPress user account, allowing unauthenticated attackers to overwrite the profile fields of arbitrary non-administrator users by submitting a public form that contains name and primary-email fields.	5.3	More Details
CVE-2026-125431	Missing Authorization vulnerability in Mamunur Rashid Food Menu – Restaurant Menu & Online Ordering for WooCommerce tlp-food-menu allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Food Menu – Restaurant Menu & Online Ordering for WooCommerce: from n/a through 6.0.7.	5.3	More Details
CVE-2026-125435	Insertion of Sensitive Information Into Sent Data vulnerability in IdeaBox Creations PowerPack Addons for Elementor powerpack-lite-for-elementor allows Retrieve Embedded Sensitive Data.This issue affects PowerPack Addons for Elementor: from n/a through 3.1.3.	5.3	More Details
CVE-2026-103361	The Payment Gateway via Valitor for WooCommerce WordPress plugin before 1.9.41 does not properly validate the authenticity of payment callbacks, relying on a verification secret that ships with a hard-coded default value used by every store that has not changed it, allowing unauthenticated attackers to forge a valid payment confirmation and mark arbitrary orders as paid.	5.3	More Details
CVE-2026-125448	Missing Authorization vulnerability in Kaliforms Kali Forms kali-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kali Forms: from n/a through 2.4.31.	5.3	More Details
CVE-2026-125746	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ProPluginsLab Back In Stock Notifier for WooCommerce back-in-stock-notifier-for-woocommerce allows Code Injection.This issue affects Back In Stock Notifier for WooCommerce: from n/a through 7.5.2.	5.3	More Details
CVE-2026-125763	Missing Authorization vulnerability in Brainstorm Force SureForms sureforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SureForms: from n/a through 2.13.0.	5.3	More Details
CVE-2026-125766	Insertion of Sensitive Information Into Sent Data vulnerability in WPZOOM WPZOOM Social Feed Widget & Block instagram-widget-by-wpzoom allows Retrieve Embedded Sensitive Data.This issue affects WPZOOM Social Feed Widget & Block: from n/a through 2.4.1.	5.3	More Details
CVE-2026-114451	The Membership Plugin WordPress plugin before 4.0.6 does not perform any authorization or CSRF check before running a schema-altering database maintenance routine, allowing unauthenticated users to convert the Membership Plugin WordPress plugin before 4.0.6's own tables to a narrower character set, which irreversibly replaces every 4-byte character (such as emoji and some CJK characters) in the membership level, discount code and payment records with a question mark.	5.3	More Details
CVE-2026-124271	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 2.8.3.	5.3	More Details
CVE-2026-125767	Insertion of Sensitive Information Into Sent Data vulnerability in NerdPress Hubbub Lite social-pug allows Retrieve Embedded Sensitive Data.This issue affects Hubbub Lite: from n/a through 1.36.3.1.	5.3	More Details
CVE-2026-125776	Missing Authorization vulnerability in Cozmoslabs Profile Builder profile-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Profile Builder: from n/a through 4.0.6.	5.3	More Details
CVE-2026-129469	Course-tencent-cloud before 2.0.2 contains an insecure direct object reference vulnerability that allows unauthenticated attackers to view other users' refund previews by supplying an order sn to /api/refund/confirm. Attackers can compute valid sn values from Sqids-encoded sequential order ids using the default key to disclose ordered items, prices, refund amounts, fees and deadlines.	5.3	More Details
CVE-2026-49236	Server-Side Request Forgery (SSRF) vulnerability in Apache XML Graphics Batik. SVG color-profile xml:base bypasses Batik external resource same-origin checks This issue affects Apache XML Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.	5.3	More Details
CVE-2026-126776	SiYuan 3.7.0 before 3.8.10 on Windows contains a path traversal vulnerability in kernel/util/webfetch.go that allows attackers to write files outside the import directory via backslash-encoded filenames. Attackers controlling a URL fetched by the MCP web_fetch or http_request tools can use %5C-encoded ..\ sequences to write chosen response bytes to directories above temp/import that are writable by the SiYuan user.	5.3	More Details
CVE-2026-89326	Origin Validation Error vulnerability in Apache XML Graphics Batik: the external resource same-origin check does not compare the URL protocol This issue affects Apache XML Graphics Batik: through 1.19. Users are recommended to upgrade to version 1.20, which fixes the issue.	5.3	More Details

CVE-2026-129480	Assimp through 6.0.6 contains a heap out-of-bounds read vulnerability in MD2Importer::InternReadFile that allows attackers to read past the file buffer via an unvalidated stored frameSize header field. Attackers can supply a crafted .md2 file loaded with a non-zero keyframe selected to crash the application or leak adjacent heap memory into the imported mesh.	5.3	More Details
CVE-2026-125046	Missing Authorization vulnerability in John-Michael L'Allier Create mediavine-create allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Create: from n/a through 3.1.1.	5.3	More Details
CVE-2026-126850	Incorrect authorization in SiteIsolation in Google Chrome on on Android prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to obtain sensitive information via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-124262	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Igor Funa Ad Inserter ad-inserter allows Code Injection.This issue affects Ad Inserter: from n/a through 2.8.19.	5.3	More Details
CVE-2026-124261	Missing Authorization vulnerability in Magepeople inc. Taxi Booking Manager for WooCommerce ecab-taxi-booking-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Taxi Booking Manager for WooCommerce: from n/a through 2.1.7.	5.3	More Details
CVE-2026-85098	A reachable assertion vulnerability in the synoscgi in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers to conduct limited denial-of-service attacks.	5.3	More Details
CVE-2026-124413	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 2.10.4.	5.3	More Details
CVE-2026-124421	Missing Authorization vulnerability in BdThemes ZoloBlocks zoloblocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ZoloBlocks: from n/a through 2.8.2.	5.3	More Details
CVE-2026-124738	A flaw was found in BusyBox. When the HTTP daemon (httpd) has pre-compressed file support enabled, authentication checks are evaluated only against the requested URL path rather than the pre-compressed file being served. A remote attacker can exploit this flaw by requesting an uncompressed file path while specifying gzip encoding, bypassing password rules configured specifically for the compressed file. This vulnerability can lead to unauthorized information disclosure of sensitive files.	5.3	More Details
CVE-2026-124993	An incorrect authorization vulnerability in the Security Advisor in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote attackers to read specific files.	5.3	More Details
CVE-2026-117487	The Flatsome WordPress theme before 3.20.13 does not perform a capability or nonce check on an AJAX action available to unauthenticated users, and does not restrict the status of the posts it returns by ID, allowing unauthenticated users to disclose the content of unpublished (draft and pending) posts.	5.3	More Details
CVE-2026-125437	Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through 1.6.13.0.	5.3	More Details
CVE-2026-126957	An integer underflow in Zephyr's IPv4 option handling allows a remote, unauthenticated attacker to read stack memory. When replying to an ICMP Echo Request that carries an IPv4 Record Route or Timestamp option, icmpv4_update_record_route() and icmpv4_update_time_stamp() in subsys/net/ip/icmpv4.c compute the length of the already recorded data as ptr - ptr_offset in uint8_t arithmetic. The attacker-controlled Pointer field is checked against the option length but not against the RFC 791 minimum (4 for Record Route, 5 for Timestamp), so a smaller value wraps the length to up to 252 bytes. net_pkt_write() then reads past the 40-byte opt_data stack buffer and up to 213 bytes of stack memory, which can include stack and heap pointers, are returned in the ICMP Echo Reply. A single packet triggers the leak and the device does not crash, so it can be repeated. Devices built with CONFIG_NET_IPV4_HDR_OPTIONS, which CONFIG_NET_IPV4_IGMP selects, are affected.	5.3	More Details
CVE-2026-125438	Missing Authorization vulnerability in Webful Creations RepairBuddy computer-repair-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RepairBuddy: from n/a through 4.1235.	5.3	More Details
CVE-2026-125439	Missing Authorization vulnerability in Kit Kit (formerly ConvertKit) convertkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kit (formerly ConvertKit): from n/a through 3.5.0.	5.3	More Details
CVE-2026-125444	Missing Authorization vulnerability in King Addons King Addons for Elementor king-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects King Addons for Elementor: from n/a through 51.1.87.	5.3	More Details
CVE-2026-	Insertion of Sensitive Information Into Sent Data vulnerability in Cozmoslabs Profile Builder profile-builder allows	5.3	More

125777	Retrieve Embedded Sensitive Data.This issue affects Profile Builder: from n/a through 4.0.6.		Details
CVE-2026-125786	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ExpressTech Quiz And Survey Master quiz-master-next allows Code Injection.This issue affects Quiz And Survey Master: from n/a through 11.3.0.	5.3	More Details
CVE-2026-126759	A flaw has been found in H3C ICG2000 Unified Communication Gateway 2023. This issue affects some unknown processing of the file /wnm/check.j of the component Web Management Module. Executing a manipulation can lead to missing authentication. The attack may be performed from remote. The exploit has been published and may be used. The researcher claims that the vendor has acknowledged receipt of the vulnerability report. No further response has been received.	5.3	More Details
CVE-2026-118409	Exposure of Sensitive Information to an Unauthorized Actor in Apache Roller 4.0 through 6.1.6 allows an unauthenticated visitor to recover the email addresses of people who left approved comments. The search index stored commenter email addresses, and the public weblog search accepted queries on that field, including wildcard queries that confirm an address one character at a time. Users are recommended to upgrade to Apache Roller 6.1.7 or later and rebuild the search index.	5.3	More Details
CVE-2026-124011	XWEB EVO 5.6.2 through 5.8.8 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain the device's eth0 MAC address and system clock by accessing sysinfo.lua, which also feeds the pre-login page. Attackers can use the disclosed MAC address and system clock values to offline derive the MAC-based daily password, enabling unauthorized authentication to the device. This product line reached it's end of service date in March 2026.	5.3	More Details
CVE-2026-64858	vulnerability-operator scans SBOMs and Images for vulnerabilities. Prior to version 0.28.16, an unauthenticated information-disclosure vulnerability exposes all vulnerability scan reports served by the operator. The /report/ HTTP endpoint mounts a raw http.FileServer over the reports directory (default /reports) with no authentication, authorization, or middleware. Any client that can reach the operator's HTTP port (default 8080) can list and download every JSON vulnerability report, disclosing CVE IDs, affected package names/versions, and container image identifiers for every workload scanned in the cluster. This issue has been patched in version 0.28.16.	5.3	More Details
CVE-2026-126288	NocoDB before 2026.06.2 contains an information disclosure vulnerability that allows unauthenticated attackers to retrieve full OAuth client records by querying the public client lookup route in oauth.controller.ts. Attackers who know or guess a client identifier can obtain the registration access token to modify or delete registrations, plus the bcrypt client secret hash and owner's internal identifier.	5.3	More Details
CVE-2026-111597	The Forminator Forms WordPress plugin before 1.58.4 does not verify that a Stripe Checkout payment has completed before returning a pending submission's after-payment response, allowing unauthenticated visitors to obtain the post-payment redirect URL and thank-you message of a payment-gated form without paying.	5.3	More Details
CVE-2026-121873	The Redirection for Contact Form 7 WordPress plugin before 3.2.16 does not verify ownership of the email address supplied through its data request form action and by default records the resulting request as already confirmed, allowing unauthenticated visitors to create verified WordPress personal data erasure or export requests for addresses they do not control.	5.3	More Details
CVE-2026-124664	The Mine CloudVod WordPress plugin before 2.6.7 does not check whether the requester is enrolled in a course, or authorised at all, before returning the course's full curriculum together with the raw content of every published lesson, allowing unauthenticated visitors to retrieve paid lesson content, such as direct video source URLs, and the passwords of password-protected lessons.	5.3	More Details
CVE-2026-126268	NocoDB before 2026.08.0 contains an IP address spoofing vulnerability that allows unauthenticated attackers to forge their recorded source IP by supplying X-Forwarded-For headers, because Express trust proxy is enabled unconditionally. Attackers can write arbitrary source addresses into audit and request logs to mislead investigations and evade the per-address public API rate limiter.	5.3	More Details
CVE-2026-119303	The NotificationX WordPress plugin before 3.3.7 does not perform any capability or nonce check on one of its REST routes, allowing unauthenticated users to update a NotificationX WordPress plugin before 3.3.7 option and to repeatedly trigger emails sent through the site's own mail server.	5.3	More Details
CVE-2026-126360	OpenTelemetry Python provides the Python API and SDK for OpenTelemetry. Prior to 1.45.2, TraceContextTextMapPropagator.extract() in opentelemetry-api can perform quadratic-time regular-expression backtracking on a malformed traceparent value containing a trace-context prefix, a long whitespace sequence, and an embedded newline. Exploitation requires an attacker-controlled carrier that preserves embedded newlines and permits a sufficiently large value, because conforming HTTP header values cannot contain embedded newlines. JSON-based carriers, including applicable MCP request metadata integrations, can preserve the required newline depending on the SDK, instrumentation, and message-size limits. Parsing on an asynchronous server's event-loop thread can consume excessive CPU and delay unrelated requests, while the advisory does not establish disclosure, modification, or code execution. This issue is fixed in version 1.45.2.	5.3	More Details
CVE-2026-	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 5.127.0 via the 'search' parameter of the cr_show_more_all_reviews and cr_show_more_reviews AJAX actions. This is due to the handlers being hooked on wp_ajax_nopriv_* without a capability check (and, in the product-page handler, with a nonce check that is behind a filter defaulting to false) while passing the visitor-supplied search string straight into get_comments() as the 'search' argument, which	5.3	More

121518	core expands into LIKE conditions over comment_author, comment_author_email, comment_author_url, comment_author_IP and comment_content. This makes it possible for unauthenticated attackers to extract review author email addresses and IP addresses — fields WordPress and WooCommerce never expose to the public — one character at a time by observing whether the returned result set matches a probed substring.		Details
CVE-2026-119034	The Schema & Structured Data for WP & AMP WordPress plugin before 1.70 does not verify that a post is publicly viewable before returning its approved comments through the review feature, allowing unauthenticated attackers to read approved comments on private, draft and password-protected posts, and to retrieve approved comments site-wide.	5.3	More Details
CVE-2026-119032	The Schema & Structured Data for WP & AMP WordPress plugin before 1.70 does not check that the importing user may edit the posts named in a settings backup, nor restrict the import to its own post types, allowing users whose role an administrator has granted access to the Schema & Structured Data for WP & AMP WordPress plugin before 1.70's settings to modify, re-author, unpublish or trash any post or page on the site and write arbitrary post meta.	5.3	More Details
CVE-2026-118418	The WP Directory Kit WordPress plugin before 1.6.3 does not restrict which database models and columns its public directory-search action may return, nor verify authorisation on it, allowing unauthenticated attackers to read other users' personal data, including email addresses and logins, and private contact-form submissions.	5.3	More Details
CVE-2026-129337	Git over HTTP lowers the required permission for pushes to read access, so that the AGit flow works, and relies on the repository's server-side hooks to enforce write access. A repository that is still being created by a migration, fork or template generation has no hooks yet, so a user with read access to it could push branches and tags during that window, or after a failed migration that left the repository in that state. Git over HTTP now refuses requests to repositories that are still being created.	5.3	More Details
CVE-2026-129152	SurveyKing 1.12.0 through 1.13.2 contains an authentication bypass vulnerability that allows unauthenticated attackers to submit survey responses because AnswerServiceImpl.saveAnswer skips login-required and survey password checks. Attackers can submit responses to protected surveys and set createBy in the request body to impersonate other users, corrupting survey results.	5.3	More Details
CVE-2026-126357	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.13.16, mount() and app.mount() can remove a dynamic mount prefix using the route-pattern length rather than the matched-prefix length, allowing a crafted path to be forwarded as a protected inner route while the outer application routes the original path. Since 4.12.21, rebuilding the forwarded URL from the decoded pathname can also convert a decoded backslash to a slash and collapse parent-directory segments, again causing the mounted application to receive a protected path. An unauthenticated client can use either applicable path transformation to reach a mounted route without authentication or authorization middleware scoped to a subpath inside the mount prefix. This issue is fixed in version 4.13.16.	5.3	More Details
CVE-2026-110016	The Data Tables Generator by Supsystic WordPress plugin before 1.15.8 does not perform any authorization or ownership check before returning the stored contents of a table, relying only on a nonce that is exposed to every anonymous visitor, allowing unauthenticated users to read the full contents of any table by its identifier, including tables that are never published anywhere on the site.	5.3	More Details
CVE-2025-71461	Zipline before 4.0.2 contains a predictable filename vulnerability that allows attackers to infer other users' upload filenames by recovering the Math.random generator state. Attackers with five consecutive gfycat-style filenames can reconstruct the random state to predict previous and future filenames until the instance restarts, exposing private uploads.	5.3	More Details
CVE-2026-128075	Nuxt is an open-source web development framework for Vue.js. From 3.0.0 until 4.6.4, Nuxt wraps non-HTTP errors thrown during server rendering with createError and incorrectly treats the result as an error deliberately exposed by the application. In production, the error page payload (__NUXT_DATA__) and JSON error response can therefore disclose the original message and data, including an upstream $fetch URL, query-string secrets, response bodies, database hosts, or similar sensitive details, regardless of what a custom error.vue renders. Errors deliberately created with createError or showError, errors returned by useFetch or useAsyncData, and server/api routes are not affected because their client-visible behavior is intentional or follows a different path. This issue is fixed in version 4.6.4.	5.3	More Details
CVE-2026-129120	C-Kermit 11.0.506 before 11.1.515 contains a RECEIVE CONFIRM bypass vulnerability that allows malicious Kermit servers to write unrequested files without prompting by abusing recursive GET root computation in ckcfns.c. Attackers can send files such as .ssh/authorized_keys or shell startup files under the current directory, which rq_under_root() accepts silently, enabling persistent access or code execution.	5.3	More Details
CVE-2026-128068	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. From 1.0.3 through 1.7.1, Rails::HTML::PermitScrubber checks SVG href and xlink:href local references with a pattern whose line-start anchor and whitespace class cause an all-whitespace value to be rescanned from each line start. An attacker who supplies HTML can cause quadratic CPU consumption when an application customizes its allowed tags to include an SVG reference element such as use and permits href or xlink:href. The default allowed tag configuration is not affected. CRuby 3.2 and later uses linear-time regular expression matching for this pattern, while CRuby 3.1 and earlier and JRuby are affected. This issue is fixed in version 1.7.2.	5.3	More Details
CVE-	The User Registration & Membership WordPress plugin before 5.3.2 does not enforce its payment-before-login		

2026-109873	restriction when a registration is submitted without a membership selection, allowing unauthenticated users to create an account on a payment-gated registration form and log in without completing payment.	5.3	More Details
CVE-2026-121853	The AppPresser WordPress plugin before 5.0.0 does not restrict access to two of its REST API endpoints, allowing unauthenticated visitors to retrieve the installed versions of AppPresser, its add-ons, several third-party AppPresser WordPress plugin before 5.0.0 and its .	5.3	More Details
CVE-2026-127958	A pull request review created through the API as a draft (`event` set to `PENDING` or left empty) was added to the pull request timeline and announced through notifications and activity feeds like a submitted review. Its body and line comments were therefore visible to everyone who can read the pull request, including anonymous visitors of a public repository, before the reviewer submitted it. Pending reviews no longer get a timeline entry or notifications until they are submitted.	5.3	More Details
CVE-2026-129131	Gameyfin before 2.6.2 contains a missing authorization vulnerability that allows unauthenticated attackers to bypass login-required mode by calling Hilla endpoints annotated with @AnonymousAllowed. Attackers can POST to synchronous endpoint methods such as GameEndpoint.sync, which LiveSubscriptionSecurity never checks, to retrieve game catalog metadata, libraries, platforms, plugins and game requests.	5.3	More Details
CVE-2026-128424	A flaw was found in Kroxylicious. The ACL authorizer's rules-file parser unquotes `matching /.../` regular-expression literals using the string unquoting rules, which strips every backslash escape. As a result, an allow rule such as `matching /orders\.v1/` is compiled as the regex `orders.v1`, which also matches unintended names such as `ordersXv1`, and character classes such as `\d` and `\w` lose their special meaning. Allow rules written with regex escapes can therefore apply to more resources than the author intended. Depending on the ACL configuration, this may allow an authenticated Kafka client to access a resource (such as read or write a topic) that should have been denied.	5.3	More Details
CVE-2026-126358	Hono is a Web application framework that provides support for any JavaScript runtime. From 4.1.4 until 4.13.16, RegExpRouter can omit wildcard middleware in three version-specific cases: since 4.13.0, middleware using the explicit default parameter pattern in /api/:tenant{[^/]+}/admin/* is not applied to a route written as /api/:tenant/admin/:id; since 4.1.4, middleware on /admin/* is not applied to a route registered as /admin* for paths under /admin/; and since 4.4.0, a request path containing an encoded line terminator can reach the not-found handler without wildcard middleware. The default SmartRouter selects RegExpRouter for most applications, and the router's registration-time coverage calculation treated the first two matching pattern pairs as different while its compiled wildcard did not match line terminators in the third case. An unauthenticated client can reach a route handler or the not-found handler without authentication or authorization middleware registered on the wildcard path. TrieRouter, LinearRouter, and PatternRouter apply the middleware in the three described cases. This issue is fixed in version 4.13.16.	5.3	More Details
CVE-2026-123698	The Security For WooCommerce WordPress plugin through 1.0.16 does not restrict access to one of its REST API routes, allowing unauthenticated users to retrieve its full settings, including configured secret keys and the hidden login URL.	5.3	More Details
CVE-2026-122061	The Event Tickets and Registration WordPress plugin before 5.30.3.1 does not correctly check whether an event displays a public attendee list before returning one of its attendees over the REST API, allowing unauthenticated users to retrieve the names of attendees of events that do not show a public attendee list.	5.3	More Details
CVE-2026-123656	The ProfilePress WordPress plugin before 4.17.6 does not correctly evaluate some of its content protection rule conditions when content is rendered outside the main query, allowing unauthenticated users to read the content of pages protected by such rules via the REST API.	5.3	More Details
CVE-2026-46676	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. From versions 1.4.0 to before 1.4.4, and 1.5.0 to before 1.5.1, an uninitialized value use vulnerability in bacnet-stack's AtomicReadFile record-access ACK encoder allows unauthenticated remote attackers to corrupt the encoded OCTET STRING length and payload boundary in network responses by sending a crafted AtomicReadFile request that reaches a successful record-access path. This issue has been patched in versions 1.4.4 and 1.5.1.	5.3	More Details
CVE-2026-126205	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Prior to 2.25.3, the Loofah HTML5 sanitizer checks href and xlink:href on elements in SVG_ALLOW_LOCAL_HREF with a regular expression whose line anchor and newline-matching whitespace cause an all-whitespace value to be rescanned from every line start. An attacker can submit an SVG reference element with a long multiline-whitespace attribute and consume CPU quadratically during sanitization. CRuby 3.1 and earlier and JRuby are affected, while CRuby 3.2 and later uses linear-time regular-expression matching. The default safelist reaches the vulnerable check without a configuration change. This issue is fixed in version 2.25.3.	5.3	More Details
CVE-2026-127206	Image CAPTCHA for Contact Form 7 and WPForms through 3.3.29 contains a CAPTCHA bypass vulnerability that allows unauthenticated attackers to defeat the anti-automation control by exploiting a hardcoded static answer in the Contact Form 7 integration. Attackers can submit kc_captcha=kc_human to pass validation in cf7ic_check_if_spam() on every protected form, enabling automated contact-form spam and abuse of actions gated only by this CAPTCHA.	5.3	More Details
CVE-2026-	NLTK from 3.2.5 before 3.10.4 contains an algorithmic complexity vulnerability in TreebankWordTokenizer.span_tokenize that allows remote attackers to cause quadratic CPU consumption through repeated list.pop(0) calls. Attackers can submit long runs of double-quote characters to services span-	5.3	More Details

126300	tokenizing untrusted text, exhausting a CPU core and degrading availability.		
CVE-2026-126343	@hono/node-server allows running the Hono application on Node.js. From 2.0.0 until 2.1.6, the WebSocket upgrade handler waits for the Hono application to finish asynchronous middleware or handler work without first attaching an error listener to the socket. If an unauthenticated client resets the TCP connection during that window, the socket emits an unhandled ECONNRESET error and terminates the Node.js process. If a global uncaughtException handler suppresses termination, the pending upgrade waiter is not released and repeated requests can grow the heap. This affects applications that enable WebSocket support and perform asynchronous work on the upgrade path. This issue is fixed in version 2.1.6.	5.3	More Details
CVE-2026-126345	basic-ftp is an FTP client for Node.js. Prior to 6.2.4, the MLSD directory-listing parser in src/parseListMLSD.ts uses untrusted fact names from the FTP server as keys in the plain-object factHandlersByName dictionary without checking that the resolved property is an own handler. A fact named __proto__ therefore resolves to Object.prototype, bypasses the missing-handler guard, and is called as though it were a function, producing a TypeError. The error propagates through Client.list() and APIs that depend on it because it is not an FTPError. A malicious or compromised FTP server, or an on-path attacker on a plaintext FTP session, can make the affected operation reject, and the Node.js process terminates under the default behavior in Node.js 15 and later only if the application leaves that rejection unhandled. This issue is fixed in version 6.2.4.	5.3	More Details
CVE-2026-123657	The ProfilePress WordPress plugin before 4.17.6 does not reject negative membership plan identifiers before checking whether a plan is active, allowing unauthenticated visitors to sign up for membership plans an administrator has deactivated and receive the role attached to them.	5.3	More Details
CVE-2026-126301	NLTK from 3.6 before 3.10.4 contains an algorithmic complexity vulnerability in LegalitySyllableTokenizer.tokenize that allows remote attackers to exhaust CPU by supplying long all-vowel tokens. Attackers can submit a token such as a long run of vowels, causing the unguarded onset reversal loop to perform quadratic work and deny service to syllabification components.	5.3	More Details
CVE-2026-126210	@hono/node-server allows running the Hono application on Node.js. Prior to 1.19.18 and from 2.0.0 until 2.1.6, the server passes a raw request-target containing a backslash in its path to the WHATWG URL parser, which treats the backslash as a path separator and resolves dot segments. A reverse proxy, load balancer, or web application firewall that preserves the backslash and applies path-based rules to the original request can therefore permit a request that the application normalizes to a blocked route. This lets an unauthenticated client reach route content that the upstream component was intended to deny, while Hono application access controls are unaffected because they operate on the normalized path. This issue is fixed in versions 1.19.18 and 2.1.6.	5.3	More Details
CVE-2026-126355	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.13.16, csrf() limits origin validation to the content types normally sent by HTML forms and therefore does not validate text/ping requests generated by Chromium hyperlink auditing. Chrome and Edge can send a cross-origin credentialed POST without a CORS preflight through an <a ping> action, and the middleware then skips both Origin and Sec-Fetch-Site checks. The fixed request body limits exploitation to state-changing endpoints whose effect is selected by the path or query string and does not depend on submitted body data. The user's cookie must accompany the request, which generally requires a same-site origin or a cookie configured with SameSite=None, and Firefox does not send hyperlink-auditing pings by default. This issue is fixed in version 4.13.16.	5.3	More Details
CVE-2026-126356	Hono is a Web application framework that provides support for any JavaScript runtime. From 4.5.1 until 4.13.16, validator('form') uses a strict whole-header pattern that fails to recognize multipart/form-data when its Content-Type includes another legal parameter or extra whitespace after a semicolon. The validation callback receives an empty object even though c.req.parseBody() or c.req.formData() can still parse and expose all submitted fields to the handler. An unauthenticated client can therefore bypass allow-list or required-field checks when the application relies on the form validator and its callback accepts an empty object. application/x-www-form-urlencoded requests are not affected. This issue is fixed in version 4.13.16.	5.3	More Details
CVE-2026-16664	MCUboot's Zephyr serial-recovery upload handler bs_upload() in boot/boot_serial/src/boot_serial.c decodes the host-supplied image field of an MCUmgr image-upload request into img_num (a full 32-bit value) and latches it on the off == 0 packet without any range check. It then passes img_num straight to flash_area_id_from_multi_image_slot(img_num, 0), which on the Zephyr port resolves to __flash_area_ids_for_slot() in boot/zephyr/include/sysflash/sysflash.h and indexes the static const int all_slots[] table as all_slots[img_num 2]. That table holds only MCUBOOT_IMAGE_NUMBER 2 entries, so any img_num >= MCUBOOT_IMAGE_NUMBER is an out-of-bounds read. The path is reachable by anyone with access to the serial / SMP recovery console, which is unauthenticated by design, and the bad value is supplied before any image signature is verified. The defect is specific to the default non-direct upload path (MCUBOOT_SERIAL_DIRECT_IMAGE_UPLOAD disabled) on the Zephyr port with the array-backed slot layout (not CONFIG_SINGLE_APPLICATION_SLOT). It is not gated on a multi-image configuration: MCUBOOT_IMAGE_NUMBER defaults to 1, so even a default single-image build is affected for any image >= 1. The MCUBOOT_SERIAL_DIRECT_IMAGE_UPLOAD path is safe (its flash_area_id_from_direct_image() switch returns -EINVAL for unknown indices). flash_area_id_from_multi_image_slot() takes a signed int image_index while img_num is uint32_t, so the attacker controls the sign of the index as well as its magnitude: an image of 0xFFFFFFFE converts to -2 and reads all_slots[-4], off the front of the table, while large positive values read off the end (CWE-192). (0xFFFFFFFF itself is the "no image given" sentinel and selects image 0.) Either way the index multiply img * 2 is performed in int, so a wild offset yields a bus/hard fault, giving a reliable denial of	5.1	More Details

	service of the bootloader during recovery. For moderately out-of-range indices the read returns adjacent .rodata as a garbage flash-area id that is handed to flash_area_open(); this normally fails with MGMT_ERR_EINVAL, but if the garbage id happens to match a valid non-image partition, the subsequent erase/write can target a partition outside the image set (CWE-787). The attacker-supplied value is never echoed back, so there is no information disclosure. The fix is to reject img_num >= BOOT_IMAGE_NUMBER on the off == 0 packet, before the slot lookup. The comparison must be made on the unsigned img_num: an equivalent guard applied after the conversion to int would not reject the negative case above. __flash_area_ids_for_slot() should bounds-check its own arguments as defence in depth. This vulnerability was reported independently twice: by NVIDIA Project Vanessa on 2026-06-22, and by Kai Phan (@kaimandalic) on 2026-07-19 as GHSA-8v33-88p6-jffj, which is closed as a duplicate of this advisory. Both original reports are reproduced in full below.		
CVE-2026-125826	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Blubrry Podcasting PowerPress Podcasting powerpress allows Path Traversal.This issue affects PowerPress Podcasting: from n/a through 11.18.3.	5.0	More Details
CVE-2026-121472	The AutomatorWP WordPress plugin before 6.0.8 does not bind the requests that complete its Zoom and AWeber integration connections to the administrator who started them, allowing attackers to make a logged-in administrator replace the stored integration credentials with the attacker's own via a CSRF attack, diverting the data the site sends to those services into an account the attacker controls. Exploitation requires the integration to already be connected and knowledge of the site's OAuth client identifier.	5.0	More Details
CVE-2026-64686	OpenSearch Dashboards is an open-source data visualization tool designed to work with OpenSearch. From versions 2.14.0 to before 2.19.6, and 3.0.0 to before 3.7.0, a Server-Side Request Forgery (SSRF) vulnerability in OpenSearch Dashboards exists in the fetchDataSourceMetaData route. The sibling test_connection route validates incoming endpoint URLs via isValidURL() against configured endpointDeniedIPs and endpointAllowlistedSuffixes lists, but fetchDataSourceMetaData accepts the same input shape without performing this validation. An authenticated user can supply an internal or loopback endpoint to probe internal network resources. This issue has been patched in versions 2.19.6 and 3.7.0.	5.0	More Details
CVE-2026-126450	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability that allows authenticated users to inject scripts by placing payloads in the patient External ID field. The payload executes when other users open the patient's prescriptions via View Printable Version (HTML), running script in their browser sessions.	5.0	More Details
CVE-2026-126770	OpsTree REMS through 1.0.0 contains a server-side request forgery vulnerability that allows authenticated users to make the backend connect to arbitrary destinations through the database Test Connection feature. Attackers can set a database entry's host and port to localhost, internal addresses, or attacker-controlled servers to probe internal hosts and ports reachable from the REMS server.	5.0	More Details
CVE-2026-128328	Dokploy 0.28.0 before 0.31.1 contains a path traversal vulnerability that allows authenticated organization members to list tracked files of any git repository by supplying an arbitrary repoPath to patch.readRepoDirectories. Attackers with read access to one service can enumerate file and directory names of other tenants' application and compose source trees on the host or managed servers.	5.0	More Details
CVE-2026-129356	A vulnerability was found in vllm-project vllm 0.30.0/0.31.0. This vulnerability affects unknown code of the file single_type_kv_cache_manager.py of the component Common Prefix Handler. The manipulation results in race condition. The attack may be performed from remote. Attacks of this nature are highly complex. It is stated that the exploitability is difficult. The exploit has been made public and could be used. Upgrading to version 0.32.0 is able to resolve this issue. The patch is identified as e687a251bb056fa527846633f7a1b0a6c0f42374. You should upgrade the affected component.	5.0	More Details
CVE-2026-86353	Dell PowerStore contains a use of a weak cryptographic algorithm vulnerability that could allow an attacker with existing privileged access to the appliance to recover stored credentials.	5.0	More Details
CVE-2026-127058	WonderCMS before 3.7.0 contains an unverified password change vulnerability in the saveAction functionality that allows an authenticated attacker to change the administrator password without re-authentication. Attackers can exploit this missing re-verification check during password changes to bypass re-authentication controls and maintain or escalate unauthorized access to the administrative account.	4.9	More Details
CVE-2026-123666	The Photo Engine (Media Organizer & Lightroom) WordPress plugin before 6.6.2 does not check that a user may delete the media in a collection before deleting it along with the collection, allowing users with the Author role and above to permanently delete other users' synced media, including administrators'.	4.9	More Details
CVE-2026-40820	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getVpnData function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	4.9	More Details
CVE-2026-126943	Zipline from 4.2.0 before 4.6.2 contains an information disclosure vulnerability that logs sensitive environment variable values, such as OAUTH_OIDC_CLIENT_SECRET, without redaction at startup. Attackers with access to system journal or docker logs can obtain OAuth2 client secrets and use them to exchange intercepted OAuth2 callbacks for valid tokens.	4.9	More Details
	The WPMR Google Feed Manager for WooCommerce – Sell on Google Merchant Center & Shopping plugin for		

CVE-2026-116614	WordPress is vulnerable to generic SQL Injection via the 'sourceId' parameter in all versions up to, and including, 2.24.1 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 editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The plugin grants the edit_feeds capability to the Editor role on activation, meaning any Editor-level user satisfies the authorization checks and can exploit this vulnerability.	4.9	More Details
CVE-2026-82179	Dell PowerStore contains an authorization bypass vulnerability. An authenticated administrator could exploit this vulnerability to bypass multi-approver controls on critical operations.	4.9	More Details
CVE-2026-126640	The WP Ultimate CSV Importer WordPress plugin before 9.3 does not escape values from imported files before using them in SQL queries when importing LifterLMS content, allowing high privilege users such as admin, including the administrator of a single site on a multisite network, to perform SQL injection attacks.	4.9	More Details
CVE-2026-63505	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Prior to version 0.223.1, Probo's console GraphQL API is a multi-tenant GRC platform where all data is scoped to an organization. A Finding can reference a Risk via finding.riskId. That reference is stored without validating that the risk belongs to the caller's organization, and the Finding.risk field resolver authorizes the finding (caller's org) instead of the risk, then loads the risk with a tenant scope derived from the risk's own global ID. As a result, an authenticated member of organization A can attach an arbitrary organization B risk GID to a finding they own and then read organization B's Risk (name, description, treatment, category, severity, owner) — with no membership in B. The stored cross-tenant reference also blocks B from deleting its own risk (ON DELETE RESTRICT), a cross-tenant integrity/DoS. This issue has been patched in version 0.223.1.	4.9	More Details
CVE-2026-128048	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 lets restricted administrators read decrypted configuration secrets because the store.getConfig email template directive's encrypted-path check missed config.xml-declared paths, case variants of the getConfig method name, and parent paths. Administrators with Transactional Emails access can preview a crafted template to expose PayPal, payment gateway, and carrier credentials.	4.9	More Details
CVE-2026-128334	listmonk 6.2.0 before 7.0.0-beta.2 contains a missing authentication vulnerability that allows unauthenticated attackers to submit Azure Event Grid bounce webhooks when no shared secret is configured. Attackers can POST forged EmailDeliveryReportReceived events with Bounced status to /webhooks/service/azure to blocklist, unsubscribe, or delete arbitrary subscribers.	4.8	More Details
CVE-2026-112201	A flaw was found in the login-failure storage component of Keycloak, the identity and access management solution. This issue specifically affects deployments using MySQL or MariaDB databases in a multi-node configuration. When multiple failed login attempts occur simultaneously for the same account, a synchronization error can cause the system to enter a repetitive loop that locks the user's record in the database. This results in legitimate login attempts for that user being blocked and failing with an error. Furthermore, because some failures are not correctly recorded during this loop, the system's brute-force protection may not accurately count all failed attempts.	4.8	More Details
CVE-2026-126296	NLTK before 3.10.4 contains a path traversal vulnerability in save_maxent_params() and load_maxent_params() that bypasses the pathsec filesystem restriction mechanism. Attackers who control the tab_dir argument can read or overwrite model parameter files outside permitted data roots, because the functions call Python's built-in open() directly.	4.8	More Details
CVE-2026-128019	FrankenPHP before 1.13.4 contains an information disclosure vulnerability in worker mode that leaks per-request environment variables into later requests on the same PHP thread. Attackers can read values set via env directives with request placeholders or WithRequestEnv() through getenv() or $_SERVER, causing applications to act on another user's routing, tenant, or authorization values.	4.8	More Details
CVE-2026-129482	OkHttp through 5.5.1 contains an improper certificate validation vulnerability in CertificatePinner that skips pin checks because Pin.matchesHostname does not normalize trailing-dot hostnames. Network attackers with a CA-trusted certificate not matching configured pins can intercept or modify TLS traffic when applications request the trailing-dot form of pinned hosts.	4.8	More Details
CVE-2026-126571	Padloc 4.0.0 before 4.3.1 contains an authentication bypass vulnerability in the legacy retrieveMFAToken handler that never counts wrong email verification codes toward the attempt limit. Unauthenticated attackers knowing a victim's email can brute force the 6-digit code to obtain verification tokens usable in signup, login and account recovery flows.	4.8	More Details
CVE-2026-115819	Calling the wide scanf family of functions (swscanf, fwscanf, wscanf, vswscanf, vfwscanf and vwscanf) with a %s or %[conversion without the 'l' length modifier in the GNU C Library version 2.2 to version 2.44 writes an extra null byte one past the end of the destination array when the converted multibyte string and its terminating null byte exactly fill that array. These conversions store each wide input character into the caller's char array as a multibyte sequence. The conversion ends with the sequence that returns to the initial shift state, which also stores the terminating null byte, and the functions then append a second null byte. A destination sized for the converted string and one terminator, as the C standard requires the caller to provide, is therefore written one byte past its end. The out-of-bounds byte is always a null byte, which may corrupt adjacent data or crash the process. An attacker who supplies the input can trigger the overflow with a string whose converted length	4.8	More Details

	exactly fills the destination. The narrow scanf functions, the %ls and %l[conversions into a wchar_t array, and the 'a' and 'm' allocation modifiers are not affected, and storing a wide scanf conversion into a narrow char array is uncommon. This issue affects all architectures and ABIs supported by the GNU C Library.		
CVE-2026-128336	ExcelJS through 4.4.0 contains a prototype pollution vulnerability that allows attackers to add numeric keys to Object.prototype through a crafted defined name referencing a __proto__ sheet. Attackers can supply an xlsx whose xl/workbook.xml definedName range targets __proto__, causing CellMatrix to write empty arrays onto Object.prototype process-wide when workbook.xlsx.load() runs.	4.8	More Details
CVE-2026-126559	Semantic MediaWiki 4.2.0 before 7.4.1 contains a stored cross-site scripting vulnerability in OptionsBuilder::profiles() that allows users with the smw-schemaedit right to inject markup. Attackers can save FACETEDSEARCH_PROFILE_SCHEMA profile keys or labels that break out of option elements, executing scripts for every Special:FacetedSearch visitor including administrators.	4.8	More Details
CVE-2026-123699	The Security For WooCommerce WordPress plugin through 1.0.16 does not check that the requester is authorised before running bulk Security For WooCommerce WordPress plugin through 1.0.16, and WordPress core updates, allowing unauthenticated users to force every pending update to be installed on the site.	4.8	More Details
CVE-2026-126477	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability in the Eye Exam (eye_mag) module that allows administrators to inject JavaScript through unencoded Eye_defaults list option titles. Attackers can store a crafted title via edit_list.php that breaks out of a jQuery string in eye_base.php, executing script in any authenticated user's session when they click Defaults.	4.8	More Details
CVE-2026-121498	The AskAny WordPress plugin before 2.2.1 does not verify that a chat session belongs to the requester before returning or changing it, allowing unauthenticated users who obtain or guess another visitor's session identifier to read that visitor's chat transcript, name, email address and IP address, and to add messages to their conversation or overwrite their details.	4.8	More Details
CVE-2026-126354	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.2.5 until 2.9.1, Addressable::URI.normalize_path can resolve a path containing leading parent segments and later parent segments to a different path than an RFC 3986 resolver. URI#normalize, URI#join, URI#==, and URI#=== inherit the result. An application that authorizes the Addressable-normalized path but sends the original URI to another resolver can allow access outside the intended path allowlist. Applications that use the same normalized value for authorization and the request, or reject parent segments, are unaffected. This issue is fixed in version 2.9.1.	4.8	More Details
CVE-2026-126407	Wasmtime before 36.0.20, 37.0.0 before 48.0.8, 49.0.0 before 49.0.5, and 50.0.0 before 50.0.1 allocates untracked host memory when a component receives a borrow of a resource it defines itself, bypassing the per-store handle limit. A malicious guest component can repeatedly transfer such borrowed resources to consume arbitrary host memory, causing denial of service.	4.8	More Details
CVE-2026-126367	@grpc/grpc-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. Before 1.13.2, and from 1.14.0 through 1.14.1, the @grpc/grpc-js-xds SafeRegexValueMatcher and PathSafeRegexValueMatcher add start and end anchors without grouping a supplied top-level alternation. An expression intended to match one of several complete values can therefore match a prefix, substring, or suffix. The affected matchers are used for route selection, xDS credential identity matching, and RBAC URL path, principal name, server name, and header rules. An ALLOW policy using an alternation can consequently accept a method, certificate identity, or header value outside the intended set, while a DENY policy becomes broader rather than permissive. This issue is fixed in versions 1.13.2 and 1.14.2.	4.8	More Details
CVE-2026-110199	IBM ContextForge MCP Gateway 1.0.0 through 1.0.11 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2026-126619	Misinterpretation of SQL statement text in the database layer of Progressive Robot hMailServer 6.0.0-B1 through 6.3.7 allows a remote unauthenticated attacker to have a failed database write reported to the server as successful. The layer answers a failed statement as a success when it finds the marker [IGNORE-ERRORS], which is meant only for the server's own schema statements (its upgrade scripts and the database log's tables), and statements carry values from outside - an envelope address, the user name of a failed logon, a message's headers - in their text on MySQL/MariaDB and PostgreSQL, and in the batches of the database log on every engine. Up to 6.2.18 the marker was honoured anywhere in a statement, a value included, on MySQL/MariaDB and PostgreSQL. From 6.2.19 it was honoured only inside a comment, but the layer read a backslash inside a string literal as an escape, which SQL Server, SQL Server Compact and PostgreSQL with standard_conforming_strings on (its default) do not, so that on those engines a value holding a backslash could make the layer take part of the statement's literals for statement text and find the marker there: on PostgreSQL from 6.3.3 for every statement carrying an outside value that holds a backslash, with no setting changed for a message delivered into a local mailbox (through an internationalised (SMTPUTF8) envelope sender) and for the IP range an auto-ban writes (named after the user name of the failed logon), and on SQL Server and SQL Server Compact for the database log, when the server logs to the database (logging is off, and the log device is files, by default). A statement run outside a transaction that then failed - a constraint, a deadlock, a lock or statement timeout, a full disk, and up to 6.2.18 a lost connection - was answered as a success, and its caller went on as if the row had been written: a message delivered into a local mailbox could be counted as delivered with no row to show it and no failure notice to its sender, and a message accepted with 250 could be left with no queue row and never delivered (up to 6.2.18, and on PostgreSQL from 6.3.3 when every recipient's address carries the	4.8	More Details

	marker too, which needs an address that takes any local part); an auto-ban whose IP range was not written could be logged and counted as applied, with no error reported, while the address stayed unbanned; and message metadata (written only when message indexing is on), entries of the database log and rows of features an administrator turns on could be lost without an error. On MySQL/MariaDB up to 6.2.18 the caller was handed whatever identifier the client library still held for the connection - 0, or that of an insert its last successful statement made, in whatever table - under which a queued message's recipients were then written, so that another message still in the queue could be delivered to them as well. This flaw gives a value no way to change what a statement does, and no privilege is gained.		
CVE-2026-128084	sqlite3 provides Ruby bindings for the SQLite3 embedded database. Prior to 2.10.2, sqlite3-ruby casts Ruby string lengths to int before passing SQL through Database#prepare, bound String or Blob values through Statement#bind_param, and String or Blob results from Ruby-defined SQL functions and aggregates through Database#create_function and Database#create_aggregate. On 64-bit platforms, a string of 4 GiB (2^32 bytes) or larger can wrap the length so SQLite processes only a prefix. A truncated SQL string can drop trailing clauses such as a WHERE condition, while a truncated bound value matters only when the application validated the full value before binding it. Exploitation requires the application and server to accept and retain the unusually large attacker-controlled string. If a dropped SQL clause contained a bind placeholder, binding raises SQLite3::RangeException instead of running the query. This issue is fixed in version 2.10.2.	4.8	More Details
CVE-2026-129247	A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.3. Impacted is the function VelocityUtils.getFileName of the file VelocityUtils.java of the component Code Generator. Performing a manipulation of the argument className results in path traversal. The attack is possible to be carried out remotely.	4.7	More Details
CVE-2026-126208	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Prior to 2.25.3, Loofah's SVG_ALLOW_LOCAL_HREF safelist lists textPath with lowercase spelling that does not match the HTML5 parser's element name and omits mpath, so external href and xlink:href values on those elements survive sanitization. Firefox fetches the attacker-chosen URL when a viewer renders the content, which can disclose the viewer's IP address, user agent, referrer, and access to hosts routable only from the viewer's network. Chrome and WebKit do not fetch these references, and the impact is a network request rather than script execution. The rails-html-sanitizer PermitScrubber reuses the affected safelist when SVG elements are permitted. This issue is fixed in version 2.25.3.	4.7	More Details
CVE-2026-128028	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a stored cross-site scripting vulnerability in Mage_Catalog_Model_Product_Option_Type_File, which accepts guest SVG, XHTML, or XML uploads through product File custom options with an empty allowed-extension list. Unauthenticated attackers can send the file URL under media/custom_options/ to victims, executing script in the store origin and exposing administrator sessions when the admin panel shares that origin.	4.7	More Details
CVE-2026-126954	Glance from 0.7.9 before 0.8.8 contains a stored cross-site scripting vulnerability that allows malicious extension endpoints to inject javascript: URLs via the Widget-Title-URL response header. Attackers controlling an extension endpoint can execute script when users click the widget title, reading dashboard pages through same-origin requests and exfiltrating content.	4.7	More Details
CVE-2026-126386	n8n before 1.123.89, 2.x before 2.45.5, 2.46.x before 2.46.1, and 3.x before 3.0.1 contains an open redirect vulnerability in the unauthenticated MCP OAuth dynamic client registration flow, which accepts arbitrary redirect_uri values via the /mcp-oauth/register endpoint. Attackers can send victims crafted /mcp-oauth/authorize URLs that redirect them to attacker-controlled sites before instance checks run, enabling phishing.	4.7	More Details
CVE-2026-128069	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. Before 1.7.2, the HTML4 and HTML5 variants of Rails::HTML::SafeListSanitizer reuse one Rails::HTML::PermitScrubber across calls and mutate its tags and attributes without synchronization. In a multithreaded process, concurrent sanitize calls using different tags: or attributes: options can interleave and cause one call to use the other call's allowlist. If a permissive call admits a script element or event-handler attribute, output expected to be sanitized under a stricter policy can retain it and cause cross-site scripting when rendered. Applications that are single-threaded, use one identical allowlist everywhere, or provide a separate scrubber: are not affected. This issue is fixed in version 1.7.2.	4.7	More Details
CVE-2026-126792	A memory-safety flaw in the key-management request-building component of the library can lead to an out-of-bounds write on the heap. A fixed-size output buffer is used under an assumption about cryptographic key size that is never validated, so when the library is embedded by a caller that supplies its own cryptographic callback implementation, data larger than the buffer can be written past its end. Exploitation requires the ability to control the embedding application's in-process key-management provider configuration, a high-privilege position. The demonstrated impact is memory corruption resulting in abnormal termination of the client process.	4.7	More Details
CVE-2026-126798	NextScan 1.1.0 through 1.2.0 contains a stored cross-site scripting vulnerability in the ns-admin URL asset detail dialog that renders crawled form request bodies (Asset_URL.data) via innerHTML without encoding. Attackers can host crafted forms on crawled sites to store JavaScript that executes when users view asset details, stealing localStorage access tokens to hijack sessions, including administrators.	4.7	More Details
CVE-2026-	Uninitialized resource in ANGLE in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	4.7	More Details

126858			
CVE-2026-126870	Uninitialized resource in ANGLE in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	4.7	More Details
CVE-2026-126871	Out of bounds read in Skia in Google Chrome on on Mac prior to 157.0.8103.78 allowed a remote attacker to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	4.7	More Details
CVE-2026-128029	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a stored cross-site scripting vulnerability in the Dataflow profile run page, which inserts catalog product import row errors into the page without escaping. Unauthenticated attackers can place markup in the store, type, or attribute_set columns of an import file to run script in the session of the administrator who imports it.	4.7	More Details
CVE-2026-126884	Out of bounds read in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	4.7	More Details
CVE-2026-128053	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a reflected cross-site scripting vulnerability in its error pages, which print SCRIPT_NAME-derived URLs built by errors/processor.php without escaping. Unauthenticated attackers can craft links that trigger uncaught exceptions on servers deriving SCRIPT_NAME from the request path, executing script in the storefront origin within victims' browsers.	4.7	More Details
CVE-2026-126207	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Prior to 2.25.3, Loofah::HTML5::Scrub.scrub_css checks only the first parse of a style attribute, then rebuilds CSS with identifier escapes decoded so escaped parentheses, property names, comments, or quotes can become a live url() without a second safety check. An attacker can use list-style to make a viewer's browser request an attacker-chosen URL when content renders, or cursor to make the request on hover. The request can disclose the viewer's IP address, user agent, access timing, and access to internal-network hosts, but no script survives sanitization and the attacker cannot read the response. This issue is fixed in version 2.25.3.	4.7	More Details
CVE-2026-86364	Dell Live Optics Collector, versions prior to 27.3.8.317 contains a Use of Insufficiently Random Values vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	4.7	More Details
CVE-2026-129094	@utcp/http before 1.1.14 contains a server-side request forgery vulnerability that allows remote manuals to reach loopback services by bypassing the remote-loopback check with a {host} placeholder. Attackers can supply host arguments like 127.0.0.1 or register tools via Streamable HTTP and SSE discovery to access internal services on the agent machine.	4.7	More Details
CVE-2026-107526	Dell PowerStore contains an improper input validation vulnerability. An authenticated low-privileged attacker could exploit this vulnerability, potentially leading to stored cross-site scripting in the management interface.	4.6	More Details
CVE-2026-126427	OpenEMR before 8.5.0 contains a session expiration vulnerability that prevents automatic logoff because the Eye Exam form's read-only poll omits skip_timeout_reset. Attackers with physical access to an unattended workstation can use the still-active session to view patient health information, since update_READONLY() resets the idle timer every 15 seconds.	4.6	More Details
CVE-2026-120407	The Contact Form 7 WordPress plugin before 6.2.5 does not restrict which user properties a form field's default value can be populated from, allowing users with the Editor role and above to obtain the password hash and sensitive user meta (such as two-factor secrets) of higher-privileged users, including administrators, who view and submit the form.	4.5	More Details
CVE-2026-114469	Out-of-bounds read can crash git-apply(1) when binary patch inflates to very large size	4.4	More Details
CVE-2026-118183	The Duplicate Post WordPress plugin before 1.5.8 does not check whether a user may publish posts when duplicating one, allowing users of a role an administrator has given Duplicate Post WordPress plugin before 1.5.8 access to, such as Contributors, to create published posts, including posts attributed to other users.	4.4	More Details
CVE-2026-120547	The CF7 Apps – Honeypot, Database, Redirection, Webhook, and Addons for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpcf7-form (CF7 form body; the [honeypot ...] tag value)' parameter in all versions up to, and including, 3.8.0 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 is only a meaningful privilege escalation on multisite installations or those with DISALLOW_UNFILTERED_HTML enabled, as Editor-level users on default single-site installs already possess the unfiltered_html capability.	4.4	More Details
CVE-2026-128241	The xmlwf tool in libexpat through 2.10.0 contains a symlink following vulnerability because -d output mode opens files with fopen("wb"), which follows symbolic links. Local attackers with write access to the output directory can plant a symlink at the expected output name to truncate or overwrite files writable by the xmlwf	4.4	More Details

	user.		
CVE-2026-128032	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 accepts the free (No Payment Information Required) payment method on orders with a non-zero total because the zero-total check runs only when payment data is imported. An API user with cart permissions can select free via cart_payment.method while the total is zero, raise it with cart_coupon.remove, and submit cart.order to place an unpaid full-price order.	4.4	More Details
CVE-2026-114466	Arbitrary data can be read or written through git-fast-import(1) and git-fast-export(1) features not marked unsafe	4.4	More Details
CVE-2026-111436	Missing release of memory after effective lifetime vulnerability in openEuler iSulad on Linux. This vulnerability is associated with program file src/daemon/modules/spec/specs_mount.c. This issue affects iSulad: through 2.1.6. The memory leak vulnerability causes the iSulad daemon to be triggered frequently, exhausting the host machine's memory and ultimately leading to an OOM crash of the daemon, resulting in a denial of service (DoS).	4.4	More Details
CVE-2026-118182	The Duplicate Post WordPress plugin before 1.5.8 does not check that a user duplicating a post is allowed to edit it, which, when the slug takeover option is enabled, allows users of a role an administrator has given Duplicate Post WordPress plugin before 1.5.8 access to, such as Contributor, to move any readable post off its permalink and publish their copy at that address.	4.4	More Details
CVE-2026-64667	pam_usb provides hardware authentication for Linux using removable media. Prior to version 0.9.3, src/local.c (pusb_get_tty_from_display_server) allocates a 4096-byte cmdline buffer, reads up to 4096 bytes from /proc//cmdline, then replaces every NUL separator with a space. When read(2) returns exactly 4096 bytes for any process the function inspects, the buffer ends without a terminator and the subsequent strstr() calls scan past the allocation boundary. The function is invoked during normal PAM authentication when DISPLAY is set, so the read fires for every process at auth time. Consequences are bounded: strstr output is a Boolean substring match (limited info-disclosure surface) but a hostile heap layout can produce a SIGSEGV that terminates the host PAM process. This issue has been patched in version 0.9.3.	4.4	More Details
CVE-2026-129127	SQLBot through 1.10.3 contains a weak password hashing vulnerability that stores local account passwords in sys_user.password as unsalted MD5 digests via md5pwd() in security.py. Attackers who obtain the user table can recover passwords, including administrator passwords, using precomputed tables or GPU cracking, since identical passwords produce identical hashes.	4.4	More Details
CVE-2026-126758	A vulnerability was detected in Moonshot AI Kimi Code up to 2.0.2. This vulnerability affects unknown code of the file .kimi-code/local.toml of the component WorkspaceDirsService. Performing a manipulation of the argument additional_dir results in reliance on untrusted inputs in a security decision. The attack requires a local approach. The exploit is now public and may be used. Upgrading to version 2.1.0 is able to resolve this issue. Upgrading the affected component is recommended.	4.4	More Details
CVE-2026-105152	Exposure of Sensitive Information to an Unauthorized Actor in Apache Roller 4.0 through 6.1.6 allows a weblog administrator to read another user's stored password hash by authoring a custom weblog template that reaches the wrapped persistent object behind the template's weblog or entry data, rather than the reduced set of fields the wrapper is meant to expose. Roller treats weblog administrators as untrusted and exposes weblog and entry data to templates only through wrapper classes, but a public accessor on those wrapper classes returned the underlying persistent object directly, including the stored password hash of the weblog's creator and of any author whose entry renders on the page. No non-default configuration is required; this affects any weblog whose administrator can author templates. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which removes template access to the underlying wrapped objects.	4.3	More Details
CVE-2026-124740	A flaw was found in BusyBox's udhcpc6 DHCPv6 client. A malicious server on the local network can trigger a use-after-free condition by responding with a crafted Dynamic Host Configuration Protocol for IPv6 (DHCPv6) reply packet lacking usable address options. This issue causes the client to read stale heap memory, which can result in a Denial of Service (DoS) due to an application crash or disclose previously assigned network address data in subsequent discovery requests.	4.3	More Details
CVE-2026-126663	Contao 4.0.0 before 5.3.54, 5.4.0 before 5.7.17, and 6.0.0 before 6.0.6 contains a path traversal vulnerability that allows content editors to read image files anywhere on the filesystem via the {{image::}} insert tag. Attackers can embed percent-encoded sequences like ..%2f that pass Validator::isInsecurePath() before rawurldecode(), making the frontend resize and serve readable image files outside the files directory.	4.3	More Details
CVE-2026-124753	Missing Authorization vulnerability in Ahmad WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through 2.7.2.	4.3	More Details
CVE-2026-128907	Missing authentication for a critical function (CWE-306) in the management service (uavmonitor_usbv1) of the 1300 communications board in DJI AeroScope Mobile (TP703) firmware 03.00.00.26, with 1300 communications board firmware 02.00.07.12 through 02.00.08.40, allows an unauthenticated attacker on the local network to read device information, such as the serial number, MAC address, IP address and radio configuration, and to change configuration settings. The service accepts commands in DJI's proprietary DUML protocol without any authentication. Exploitation requires network access to TCP port 16000 on the board and that the unit is not connected to another controlling host. The same commands are also accepted over the USB operator port.	4.3	More Details

	Confirmed on a physical device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. DJI has discontinued AeroScope Mobile and no fixed firmware is available.		
CVE-2026-125617	`GET /api/v1/users/{username}/orgs/{org}/permissions` only checked that the organization is visible to the caller and then returned the named user's role in it. Any signed-in user could learn whether another user is an owner, admin or member of a public or limited organization, including for members who conceal their membership. The roles are now only returned to the user themselves, to members of the organization and to site administrators.	4.3	More Details
CVE-2026-82014	Any authenticated user, including a Viewer, could change the preferences of any team, such as its home dashboard, theme and timezone, through an undocumented endpoint with no access control, and so redirect every member of that team to a dashboard of their choice (missing authorization).	4.3	More Details
CVE-2026-125834	Missing Authorization vulnerability in WP Media Imagify imagify allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Imagify: from n/a through 2.3.4.	4.3	More Details
CVE-2026-123661	The ProfilePress WordPress plugin before 4.17.4 does not check that a membership plan is still active when checkout is used to change an existing subscription, allowing subscribers holding any subscription of their own to subscribe to plans the site owner has deactivated, including free plans that grant a user role.	4.3	More Details
CVE-2026-123642	The AGit flow (pushing to `refs/for/...`) did not check the pusher's access to pull requests again when it created the pull request. A user or deploy key with read access to the code only, or with write access to the wiki over SSH, could open pull requests in a repository where they have no access to pull requests. Creating a pull request through AGit now requires read access to the pull requests of the repository and is refused for wiki pushes.	4.3	More Details
CVE-2026-123009	When a file is edited in a fork through the web editor, Gitea can first copy a branch from the base repository into the fork. That copy did not check whether the user may read the base repository's code. A user who had forked a repository and later lost access to it, for example after it was made private or they were removed as a collaborator, could keep copying its current branches into their fork and read them. The copy now requires read access to the code of the base repository.	4.3	More Details
CVE-2026-126496	1Panel-dev CordysCRM before 1.9.6 contains an authorization bypass vulnerability in CustomerContactController.get that allows authenticated users to read other users' contacts because no organization, owner or data-scope check is applied. Attackers holding ordinary contact or customer read permission can request GET /account/contact/get/{id} with another contact's ID to obtain names, phone numbers, owners, departments, linked customers and custom fields.	4.3	More Details
CVE-2026-126544	WWBN AVideo 6.5 through 29.7.1 contains an email verification bypass vulnerability in User::verifyCode() in objects/user.php caused by PHP loose comparison of the recoverPass token. Registered users can reuse the installation-wide salt from their own verification link and craft a code with arbitrary users_id and recoverPass set to true to verify other accounts' emails, unlocking features such as live streaming.	4.3	More Details
CVE-2026-124412	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in eLightUp Slim SEO slim-seo allows Code Injection.This issue affects Slim SEO: from n/a through 4.11.5.	4.3	More Details
CVE-2026-125778	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in myCred myCred mycred allows Code Injection.This issue affects myCred: from n/a through 4.0.2.	4.3	More Details
CVE-2026-126545	WWBN AVideo through 29.7.1 contains a missing authorization vulnerability in API::get_api_tags() in plugin/API/API.php that allows registered users to access restricted video data by querying the tags API. Attackers can subscribe to a tag and query APIName=tags to obtain filenames, titles and stored video_password values of unlisted, group-restricted and password-protected videos, enabling unauthorized viewing.	4.3	More Details
CVE-2026-118405	Exposure of Sensitive Information to an Unauthorized Actor in Apache Roller 4.0 through 6.1.6 allows any logged-in user to learn other users' email addresses. The user search in the authoring interface shows only user names, but it also matched the search text against email addresses, so a user could confirm an address one character at a time. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which matches only user names for users who are not administrators.	4.3	More Details
CVE-2026-126546	Viber for iOS through 29.4.0.24 fails to validate the logical screen width and height in received GIF headers, allowing attackers to crash the app. Attackers can send a crafted GIF with zero dimensions that triggers an uncaught NSInternalInconsistencyException, aborting the app with SIGABRT when opened.	4.3	More Details
CVE-2026-123481	Missing Authorization vulnerability in WP Extended The Ultimate WordPress Toolkit – WP Extended wpextended allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Ultimate WordPress Toolkit – WP Extended: from n/a through 3.4.2.	4.3	More Details
CVE-2026-126565	Semantic MediaWiki 3.0.0 before 7.4.1 contains a denial of service vulnerability in the ElasticStore and SPARQLStore ConceptDescriptionInterpreter classes, which re-expand concepts without memoization or an expansion budget. Users with page-edit rights can build acyclic chains of Concept: pages that fan out, so queries via concept page views, Special:Ask, or api.php action=ask exhaust CPU and memory.	4.3	More Details

CVE-2026-126562	Semantic MediaWiki 3.0.0 before 7.4.1 contains an uncontrolled recursion vulnerability in the ElasticStore ConceptDescriptionInterpreter that only detects directly self-referencing concepts. Users with page-edit rights can create mutually referencing concept pages, causing concept page views, Special:Ask, or api.php action=ask queries to exhaust PHP memory or stack.	4.3	More Details
CVE-2026-109871	The User Registration & Membership WordPress plugin before 5.3.2 does not verify that a payment has actually been completed before extending a paid membership subscription, allowing authenticated users with an active paid subscription to renew it indefinitely without paying.	4.3	More Details
CVE-2026-124269	Missing Authorization vulnerability in weDevs Happy Addons for Elementor happy-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Happy Addons for Elementor: from n/a through 3.51.0.	4.3	More Details
CVE-2026-124416	Missing Authorization vulnerability in Ahmad WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through 2.7.2.	4.3	More Details
CVE-2026-124417	Missing Authorization vulnerability in Ahmad WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through 2.7.2.	4.3	More Details
CVE-2026-125810	Missing Authorization vulnerability in myCred myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through 4.0.2.	4.3	More Details
CVE-2026-117523	The Dynific Addons for Elementor (formerly Anywhere Elementor) WordPress plugin before 1.3.1 does not perform a capability or nonce check on an AJAX action that saves its module configuration, allowing any authenticated user, including Subscribers, to enable or disable the Dynific Addons for Elementor (formerly Anywhere Elementor) WordPress plugin before 1.3.1's modules site-wide.	4.3	More Details
CVE-2026-125445	Cross-Site Request Forgery (CSRF) vulnerability in Infomaniak Network VOD Infomaniak vod-infomaniak allows Cross Site Request Forgery.This issue affects VOD Infomaniak: from n/a through 1.5.16.	4.3	More Details
CVE-2026-125436	Missing Authorization vulnerability in Mamunur Rashid The Post Grid the-post-grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Post Grid: from n/a through 7.9.9.	4.3	More Details
CVE-2026-125782	Missing Authorization vulnerability in Blubrry Podcasting PowerPress Podcasting powerpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PowerPress Podcasting: from n/a through 11.18.2.	4.3	More Details
CVE-2026-126318	REDAXO before 5.21.6 contains an authorization bypass vulnerability that allows editors without the version[live_version] permission to modify live article versions by bypassing working version enforcement. Authenticated editors can add, edit, delete, toggle, or reorder live slices via content/functions, slice ids, content_slice_status, content_move_slice, history restore, or content_copy, bypassing approval workflows.	4.3	More Details
CVE-2026-116321	Improper null termination in PostgreSQL array element assignment allows a database user to disclose server memory, via changing the final byte of a fixed-length name value to a nonzero byte and passing it to code that treats the value as a C string. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	4.3	More Details
CVE-2026-126464	OpenEMR before 8.5.0 contains a server-side request forgery vulnerability in PatientPortalPDFDocumentCreator::createPdfObject() that allows authenticated patients to make the server issue HTTP GET requests. Attackers can submit img src, inline style url(), or reinserted unpurified style blocks via the content parameter of portal/lib/doc_lib.php to probe internal ports and cloud metadata endpoints.	4.3	More Details
CVE-2026-126348	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.0.0 until 2.9.1, the pure-Ruby Addressable::IDNA.to_unicode implementation decodes invalid Punycode A-labels instead of returning them unchanged. Labels that decode to ASCII text or fail to convert back to the same A-label can therefore make Addressable::URI#display_uri show a trusted-looking host while host, normalized_host, and the connection target retain the attacker-controlled encoded host. A trusted-name comparison using Addressable::IDNA.to_unicode output can also treat two different hosts as the same without displaying the URI. The native libidn implementation, to_ascii, and normalized_host are unaffected. This issue is fixed in version 2.9.1.	4.3	More Details
CVE-2026-86324	A flaw was found in Foreman’s Api::V2::SshKeysController, where the target user is resolved through Foreman::Controller::UserAware#find_user using User.find(params[:user_id]) without enforcing the required parent-user authorization check. An attacker with the create_ssh_keys permission can exploit this authorization bypass by submitting POST /api/v2/users/:user_id/ssh_keys with another user’s ID and injecting their own public SSH key into the targeted account. The injected key is subsequently propagated to hosts provisioned by that user, potentially allowing the attacker to authenticate to and gain SSH access to the victim’s managed hosts.	4.3	More Details
	A flaw was found in Foreman’s Api::V2::MailNotificationsController, where authorization checks on user-specific mail-notification resources are insufficient. The GET /api/v2/users/:id/mail_notifications endpoint resolves the		

CVE-2026-86323	target account using User.find(params[:id]) without verifying that the authenticated user is authorized to access that user's notification configuration. Additionally, the POST and PUT /api/v2/users/:user_id/mail_notifications paths call deny_access when the requester is unauthorized but fail to halt execution, allowing the request to continue and persist the unauthorized change despite a 403 response or subsequent DoubleRenderError. This can allow a user to disclose another user's mail-notification configuration, including mail_query values, and, where write permissions apply, modify or create notification settings for another user.	4.3	More Details
CVE-2026-126438	OpenEMR before 8.5.0 contains an improper authorization vulnerability in interface/patient_file/rules/patient_data.php that allows read-only patients/med users to modify clinical-rule records. Attackers can submit a global form_entryID row ID to overwrite completion date, state, and result, including records of patients outside their configured squad.	4.3	More Details
CVE-2026-127120	A vulnerability was found in Governikus AusweisApp Mobile up to 2.5.5. This impacts an unknown function of the component StartPAOSResponse Handler. Performing a manipulation of the argument ResultMessage results in cross site scripting. The attack can be initiated remotely. Upgrading to version 2.6.0 will fix this issue. Upgrading the affected component is advised. This CVE was requested by the vendor.	4.3	More Details
CVE-2026-126445	OpenEMR before 8.5.0 contains a missing authorization vulnerability that allows any authenticated core user to modify arbitrary Patient Flow Board trackers without the patients/appt permission. Attackers can submit a victim tracker_id to patient_tracker_status.php or drug_screen_completed.php to falsify check-in status, rooms, drug-screen completion, and tracker history.	4.3	More Details
CVE-2026-126446	OpenEMR before 8.5.0 contains a missing authorization vulnerability that allows any authenticated core user to retrieve destroyed-drug records because destroyed_drugs_report.php lacks the admin/drugs or inventory/reporting ACL check. Attackers can submit the report refresh form with a chosen date range to obtain drug names, NDC, lots, quantities, destruction methods, witnesses, and notes.	4.3	More Details
CVE-2026-126448	OpenEMR before 8.5.0 contains a missing authorization vulnerability that allows authenticated users lacking nationnotes/nn_configure to modify shared Nation Notes templates by calling mutation endpoints directly. Attackers can send requests to ajax_code.php or add_context.php, which lack ACL and CSRF checks, to tamper with clinical-note templates and assignments.	4.3	More Details
CVE-2026-70642	ToolJet before 3.21.94, fixed in commit e5f387a, contains an authorization bypass vulnerability in the app environments init endpoint that allows authenticated users to read app version metadata belonging to other workspaces. Attackers can send GET requests to /api/app-environments/init with an editing_version_id from another workspace to retrieve the version name, description, status, current environment ID, and app ID, because the lookup is not scoped to the caller's organization.	4.3	More Details
CVE-2026-127145	SOGo before 5.12.13 contains a server-side request forgery vulnerability that allows authenticated users to make the server connect to arbitrary internal host:port destinations by supplying a user-controlled URL to the Calendar/addWebCalendar endpoint. Attackers can trigger a reload of the subscribed web calendar via the reload endpoint and distinguish response outcomes such as connection failures, timeouts, authentication prompts, or invalid content to probe the internal network from the server's position.	4.3	More Details
CVE-2026-124652	The Mine CloudVod WordPress plugin before 2.6.6 does not verify that an order belongs to the requesting user before returning its payment status, allowing any authenticated user, such as subscriber, to read other customers' order status, the purchased item and, while an Alipay payment is in progress, the buyer's Alipay account identifier.	4.3	More Details
CVE-2026-127135	SOGo before 5.12.13 contains a Sieve script injection vulnerability that allows authenticated users to inject arbitrary Sieve directives by inserting unescaped notification address values into a generated Sieve script. Attackers can embed Sieve redirect or discard statements within the notificationAddress preference to bypass the administrator-configured forwarding-domain constraint and redirect or discard incoming mail.	4.3	More Details
CVE-2026-120154	Improper protection in PostgreSQL INSERT ... ON CONFLICT allows an attacker having INSERT, UPDATE, and applicable SELECT privileges on the table to read every row despite row security policies, via iterated INSERT ... ON CONFLICT DO UPDATE. Unlike CVE-2026-16237, this does not facilitate improper writes. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	4.3	More Details
CVE-2026-120152	Use after free in PostgreSQL pg_show_all_settings() allows a database user to retrieve memory contents, via loading a module while the function is scanning custom-variable placeholders that the module replaces and frees. Within major versions 16-18, minor versions before PostgreSQL 18.7, 17.12, and 16.16 are affected. Versions before PostgreSQL 16 are unaffected.	4.3	More Details
CVE-2026-120146	Missing authorization in PostgreSQL REASSIGN OWNED allows a role granted INHERIT but not SET to transfer objects to the granted role. It also allows reassignment of database ownership without the CREATEDB privilege. The equivalent ALTER ... OWNER commands block this. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	4.3	More Details
CVE-2026-116327	Exposure of sensitive information in PostgreSQL security_barrier processing allows a database user to infer values hidden by a security_barrier view, via applying a leaky function to a CASE test value or internal parameter that indirectly represents a protected column. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	4.3	More Details

CVE-2026-126766	OpsTree REMS through 1.0.0 contains an improper authorization vulnerability that allows authenticated users to set an incident's reporter to another user by supplying a client-controlled reporter field. Attackers can send crafted POST /api/v1/incidents or PATCH /api/v1/incidents/{id}/status requests to falsify incident attribution and corrupt the accountability audit trail.	4.3	More Details
CVE-2026-116310	Use after free in PostgreSQL COPY FROM error reporting allows a database user to disclose portions of server memory, via a longer input row following an ignored or nullified conversion error. file_fdw reaches the same code path in affected version 18. Within major versions 17-18, minor versions before PostgreSQL 18.7 and 17.12 are affected. Versions before PostgreSQL 17 are unaffected.	4.3	More Details
CVE-2026-116308	Buffer over-read in PostgreSQL dict_int allows a database user to disclose portions of server memory, via a zero-length token. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	4.3	More Details
CVE-2026-71367	An incorrect authorization vulnerability was found in AWX's WebSocket consumer. The consumer_access() function only enforces access controls for object-level event groups (job_events, workflow_events, ad_hoc_command_events) but does not restrict subscriptions to global broadcast groups such as 'jobs-status_changed'. When an authenticated user subscribes to a global broadcast group, the server accepts the subscription without verifying that the user has permission to view the associated resources. In multi-organization deployments, this allows a low-privilege user in one organization to receive real-time job status metadata from all organizations, including job IDs, status transitions, timestamps, and infrastructure topology details such as instance group names, bypassing the organization isolation enforced by the REST API.	4.3	More Details
CVE-2026-126426	OpenEMR 5.0.2 before 8.5.0 contains a missing authentication vulnerability in mfa_registrations.php and mfa_u2f.php that allows session hijackers to delete MFA factors or register U2F keys without password re-entry. Attackers holding a victim's authenticated session can remove all second factors or add their own U2F key, bypassing MFA at later logins with the password.	4.3	More Details
CVE-2026-126423	OpenEMR before 8.5.0 contains a denial of service vulnerability in four ZIP upload paths that read uncompressed entries into memory without size or ratio checks. Authenticated billing or Carecoordination users can upload highly compressed ZIP archives to exhaust PHP memory and worker pools, making OpenEMR unavailable.	4.3	More Details
CVE-2026-126422	OpenEMR before 8.5.0 contains a missing authorization vulnerability in library/ajax/lists_touch.php that allows restricted authenticated users to mark another patient's clinical lists as reviewed. Attackers can submit arbitrary patient_id and type values to falsely record "None known" allergy, medication, or problem lists, misleading clinicians and skewing quality-measure calculations.	4.3	More Details
CVE-2026-126421	OpenEMR before 8.5.0 contains an uncontrolled resource consumption vulnerability that allows authenticated users with patients/med access to exhaust PHP workers via an unbounded count parameter. Attackers can send print_labels requests to labs_ajax.php with huge counts, forcing mPDF page and barcode generation that makes OpenEMR unavailable.	4.3	More Details
CVE-2026-126323	Vvveb through 1.0.8.6 contains a cross-site request forgery vulnerability that allows attackers to perform admin state-changing actions because checkCsrf() in admin/controller/base.php only validates tokens for POST requests. Attackers can lure a logged-in admin into loading a forged cross-site GET request to delete admin/user accounts, sites, orders, and menus or change comment status.	4.3	More Details
CVE-2026-126292	NocoDB before 2026.06.1 contains an information disclosure vulnerability in the profile update handler in users.service.ts, which returns the stored user record without passing it through the user-serialization filter, exposing the bcrypt password hash, salt, and session token counter. Attackers holding a stolen or hijacked session can update the profile to retrieve that account's password hash and salt for offline cracking.	4.3	More Details
CVE-2026-126373	Vvveb 1.0.8.4 through 1.0.8.6 contains an authorization bypass vulnerability in the content/revisions revision action that lets low-privileged Authors read other authors' revisions. Attackers can supply a post_id, language_id, and created_at timestamp to retrieve private unpublished drafts, because the revision() action lacks the admin_id ownership restriction.	4.3	More Details
CVE-2026-126374	Vvveb through 1.0.8.6 contains an SQL injection vulnerability because the @KEYS(:each) macro emits PHP array keys as backtick-quoted INSERT column names without escaping, and several procedures in admin/sql/mysqli/product.sql and admin_auth_token.sql omit the @FILTER guard. Authenticated back-office users able to save products can submit product_<feature> POST array keys containing backticks to redirect bound values into unexposed columns or break SQL statements.	4.3	More Details
CVE-2026-116433	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	4.3	More Details
CVE-2026-82174	Dell PowerStore contains a content-injection vulnerability. An unauthenticated attacker could exploit this vulnerability to display misleading text on the genuine login page for phishing.	4.3	More Details
CVE-2026-116436	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	4.3	More Details

CVE-2026-116431	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains a Cleartext Storage of Sensitive Information vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	4.3	More Details
CVE-2026-116430	Dell PowerScale InsightIQ, Version 6.4.0, contain an Insufficient Verification of Data Authenticity vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering.	4.3	More Details
CVE-2026-116426	Dell PowerScale InsightIQ, Versions 6.3.0 through 6.4.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	4.3	More Details
CVE-2026-116432	Dell PowerScale InsightIQ, versions 6.3.0 through 6.4.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	4.3	More Details
CVE-2026-123670	The Essential Real Estate WordPress plugin before 5.3.6 does not verify that the recipients it allows for its contact email action are legitimate, allowing users with the self-registered Customer role to add any address to that allowlist so that unauthenticated users can then send emails with attacker-controlled content to it through the site.	4.3	More Details
CVE-2026-123093	The WP Remote Users Sync WordPress plugin before 2.2.1 does not have authorisation and CSRF checks in one of its AJAX actions, allowing any authenticated user, such as a subscriber, to delete the WP Remote Users Sync WordPress plugin before 2.2.1's entire activity log.	4.3	More Details
CVE-2026-127285	A flaw has been found in Cairo-dock Glx-Dock 3.4.0. The affected element is an unknown function of the file bg_forum.php of the component href Attribute Handler. This manipulation of the argument f causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-127282	A vulnerability was determined in SourceCodester Smart Attendance System with QR Code Scanner 1.0. Affected by this vulnerability is an unknown functionality of the file reset_password.php. This manipulation of the argument Username causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-126413	Frappe HRMS 15.x before 15.64.1 and 16.x before 16.19.0 contains a missing authorization vulnerability in an endpoint that returns file information, allowing authenticated users to read details of files attached to records they cannot access. Any logged-in user, including one with only the Employee role, can query it to view attachment details on any document type and confirm record existence.	4.3	More Details
CVE-2026-129157	ragent 1.0.0 through 1.1.0 contains a missing authorization vulnerability in RagTraceController that allows any logged-in user to view all users' RAG traces. Attackers can page through /rag/traces/runs and related node endpoints to read other users' usernames, user ids, conversation ids, questions, and per-node execution details.	4.3	More Details
CVE-2026-127273	A vulnerability has been found in Linksys EA8100 1.0.3.216940. This affects the function GetWANStatus/GetWANStatus3/IsAdminPasswordDefault of the component JNAP API. The manipulation leads to missing authentication. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-127212	Dokploy before 0.31.1 contains a missing ownership check vulnerability in the readAppMonitoring tRPC procedure that allows authenticated attackers to access container metrics belonging to other organizations by supplying an arbitrary appName. Attackers can query getApplicationStats with any application name, including the fixed "dokploy" control-plane service name, to read CPU, memory, network I/O, and block I/O metrics for containers they do not own on self-hosted multi-tenant instances.	4.3	More Details
CVE-2026-126485	OpenEMR before 8.5.0 contains a cross-site request forgery vulnerability in ObservationController::deleteAction that allows attackers to delete observation form records without a CSRF token. Attackers can lure a logged-in clinician to a page issuing a GET to delete.php with guessed id values, soft-deleting observations in the victim's open encounter.	4.3	More Details
CVE-2026-126898	Uninitialized resource in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-126757	A security vulnerability has been detected in Moonshot AI Kimi Code up to 2.5.2. This affects the function isOriginAllowed of the file apps/kimi-code/dist-web/assets/index-HU0LCM-X.js of the component Web UI. Such manipulation of the argument kimi_origin leads to open redirect. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-126857	Out of bounds read in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details

CVE-2026-126932	Zipline 4.6.2 before 4.8.0 contains a policy bypass vulnerability that allows authenticated users to evade administrator-disabled MIME types by editing file metadata. Attackers can upload a permitted file, then set a disabled type such as text/html through PATCH /api/user/files/:id so /raw/:id serves that Content-Type.	4.3	More Details
CVE-2026-126920	Information leak in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-126914	Uninitialized resource in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-126313	Frappe HRMS 16.0.0 before 16.20.1 contains an authorization bypass because an ownership check is missing on a record type that employees can create. Authenticated users holding only the Employee role can create or change draft records for another employee, or for a company they do not belong to.	4.3	More Details
CVE-2026-126891	Use after free in V8 in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to read memory inside the sandbox via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-126878	Information leak in Core in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-64861	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Prior to version 0.222.0, the GraphQL endpoint does not enforce restrictions on alias count, query depth, or query complexity. An attacker can send a single request containing thousands of aliased resolver calls, causing excessive server-side resource consumption and service degradation. This issue has been patched in version 0.222.0.	4.3	More Details
CVE-2026-126856	Incomplete cleanup in Cache in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-126808	weDevs ERP (WP ERP) through 1.17.11 contains an incorrect authorization vulnerability that allows authenticated employees to edit their own HR records because HRM AJAX handlers check erp_edit_employee instead of erp_manage_jobinfo. Attackers can post their own user_id with the My Profile nonce to change designation, reporting manager, pay rate, and employment type, or delete job history.	4.3	More Details
CVE-2026-126854	Incorrect authorization in Layout in Google Chrome prior to 157.0.8103.78 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-129468	Netcccyun dnsmgr 2.18 before 2.22 contains a missing authorization vulnerability in POST /cloudflare/get_domain_default_line that allows restricted users to access domains outside their permissions. Restricted sub-users or single-domain logins can iterate the domain_id parameter to enumerate panel domain ids and read each domain's DNS line list and default line.	4.3	More Details
CVE-2026-129467	GeoPulse 1.5.0 through 2.3.0 contains an insecure direct object reference vulnerability in GET /api/v1/places/geocoding/{id} that allows authenticated users to read other users' private locations. Attackers can enumerate sequential reverse_geocoding_location ids to retrieve other users' custom place names, city, country, coordinates and bounding boxes from their history.	4.3	More Details
CVE-2026-124671	The Burst Statistics WordPress plugin before 3.7.5 does not enforce a shared report's date range on the analytics it serves to the report's share link, allowing anyone holding the link to read the report's statistics for any period the site retains rather than the period the report was shared for.	4.3	More Details
CVE-2026-126784	Missing rate limiting, per-account submission quota and geographic validation in the publicar_aviso RPC function in Lagarto Chivato 0.4.1 and earlier on Web allows remote authenticated attackers to flood the moderation queue via unlimited submission of notices with arbitrary coordinates.	4.3	More Details
CVE-2026-128033	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains an information disclosure vulnerability in Mage_Rss_Model_Resource_Order::getAllCommentCollection(), which omits the is_visible_on_front filter for invoice, shipment and credit-memo comments. Authenticated customers can open the /rss/order/status feed for their order to read internal staff comments, such as fraud-review and payment notes.	4.3	More Details
CVE-2026-126807	WuzAPI through 1.1.0 contains a cross-tenant information disclosure vulnerability in the GetHistory handler that allows authenticated users to view other tenants' chat metadata. Attackers with message history enabled can request GET /chat/history with chat_jid=index to list every user's internal ID, stored chat JIDs, and last-message times.	4.3	More Details
CVE-2026-	Zipline 4.0.0 before 4.8.0 contains an upload filter bypass vulnerability that allows users with upload access to store blocked file types due to extension format mismatch. The upload and partial handlers compare dotted,	4.3	More

126933	case-sensitive extensions against undotted disabledExtensions entries, letting authenticated or permitted unauthenticated folder uploaders bypass administrator restrictions.		Details
CVE-2026-127085	Ryot before 10.5.6 contains an authorization bypass vulnerability that allows authenticated users to remove entries from other users' collections by supplying arbitrary collectionName and creatorUserId values. Attackers can obtain user ids from the usersList query and target fixed collection names like Watchlist to delete collection_to_entity rows belonging to other users.	4.3	More Details
CVE-2026-74850	An improper limitation of a pathname to a restricted directory vulnerability in the contentextract in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read specific files.	4.3	More Details
CVE-2026-129254	A flaw has been found in Opixido OCMS up to b7c15660aba83d96677c1a9abaa69c082a24f21c. This impacts an unknown function of the file admin/TUI/index.php of the component Admin TUI. This manipulation of the argument img causes cross site scripting. The attack can be initiated remotely. The exploit has been published and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-126767	OpsTree REMS through 1.0.0 contains a prompt injection vulnerability that allows authenticated users to disclose the hidden system prompt by submitting crafted chat input to POST /api/v1/rca/chat. Attackers can instruct the assistant to ignore its rules and reveal internal orchestration instructions, aiding the crafting of further prompt injection attacks.	4.3	More Details
CVE-2026-126772	OpsTree REMS through 1.0.0 contains an improper attribution vulnerability that allows authenticated users to post comments as the incident creator via POST /api/v1/incidents/{incident_id}/comment. Lower-privileged attackers can comment on incidents owned by users such as a Super User to impersonate them and corrupt the incident timeline and audit trail.	4.3	More Details
CVE-2026-111034	The Countdown, Coming Soon, Maintenance WordPress plugin through 3.0.8 does not check that the user is allowed to browse content before returning post titles from one of its AJAX actions, allowing any authenticated user, such as a subscriber, to list the titles of published entries of any post type, including types that WordPress does not expose to them. Draft, private and pending content is not returned; only published entries are disclosed.	4.3	More Details
CVE-2026-88266	An external control of system or configuration setting vulnerability in the synomount in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write specific files.	4.3	More Details
CVE-2026-81559	A missing authorization vulnerability in the TaskScheduler API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write specific files.	4.3	More Details
CVE-2026-81558	A missing authorization vulnerability in the SocketIo API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write specific files.	4.3	More Details
CVE-2026-77738	A server-side request forgery vulnerability in the Credential API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to read specific files.	4.3	More Details
CVE-2026-129466	Zr.Admin.NET commit 1845017 through commit eb9228a contains a missing authorization vulnerability in TasksController.Get that allows any logged-in user to read scheduled task details without the monitor:job permission. Attackers can obtain task ids from the unprotected /monitor/jobLog/list endpoint and retrieve job parameters, API URLs, cron expressions, and stored SQL statements.	4.3	More Details
CVE-2026-19414	A missing authorization vulnerability in the Promotion API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1 allows remote authenticated users to write specific files.	4.3	More Details
CVE-2026-127074	OpsTree BuildPiper before 2.7.0 contains a path traversal vulnerability that allows authenticated users with build configuration permission to read files on the build worker by supplying unvalidated dockerfile_path and build context values. Attackers can set traversal or absolute paths such as /etc/passwd via the CI configuration endpoint, then trigger a build to disclose file contents in the build log.	4.3	More Details
CVE-2026-127081	OpsTree BuildPiper before 2.7.0 contains an authorization bypass vulnerability that allows authenticated users to link pipeline stages to environments of other projects by supplying a foreign project_env_id. Attackers can submit another project's environment identifier to the POST /api/v1/pipeline/{pipeline_id}/stages/ endpoint, persisting cross-project associations that bypass project separation.	4.3	More Details
CVE-2026-129248	A weakness has been identified in Akaunting up to 3.3.0. The affected element is the function calculation_to_quantity of the file helpers.php of the component Invoice Item Validation. Executing a manipulation of the argument quantity can lead to numeric range comparison without minimum check. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not	4.3	More Details

	respond in any way.		
CVE-2026-126775	Social-auth-core 4.7.0 before 7.0.0 contains a login cross-site request forgery vulnerability in the SAML backend that restores sessions named in the unsigned RelayState parameter. Attackers can deliver their own valid IdP response and RelayState to a victim's browser via an auto-submitting form, signing the victim into the attacker's account to capture entered data.	4.2	More Details
CVE-2026-129132	MRBS before 1.13.0 contains an LDAP injection vulnerability in web/lib/MRBS/Auth/AuthLdap.php that interpolates unescaped login usernames into DN search and group-membership filters. Attackers with valid directory credentials outside the required group can submit crafted usernames that make the group filter always true, bypassing access restrictions.	4.2	More Details
CVE-2026-128348	ExcelJS through 4.4.0 contains a formula injection vulnerability in the totals row formula getter in lib/doc/table.js that fails to escape [,], # and ' characters in structured reference column names. Attackers can supply column names containing] via untrusted input like imported CSV headers to inject formulas such as HYPERLINK that exfiltrate cell values when users open and click the generated workbook.	4.2	More Details
CVE-2026-128330	Miniflux before 2.3.5 contains an insufficient session expiration vulnerability that allows attackers to retain account access because password changes do not revoke existing web sessions. Attackers holding a leaked password or copied session cookie keep access for up to 30 days, reading integration credentials, creating API keys, or registering passkeys.	4.2	More Details
CVE-2025-71460	Zipline before 4.2.1 contains a missing authorization vulnerability in the /api/user/files/transaction endpoint that allows authenticated users to modify other users' files due to absent ownership checks. Attackers who know a target file ID can submit transaction requests to edit or delete files belonging to any user.	4.2	More Details
CVE-2026-123867	A per-host mutual-TLS authorization bypass in Node.js lets a client authorized for the default hostname reach a protected hostname it is not authorized for. When a TLS server assigns a hostname a different client-certificate CA with `server.addContext(host, { ca: protectedCA })` but no server certificate in that SNI context, the per-host client CA is never installed and the handshake falls back to the default client CA. In `src/crypto/crypto_tls.cc`, `CertCbDone` installs the SNI context's CA only when `setSniContext` succeeds, but `setSniContext` returns `false` for a context with no server certificate, so a CA-only SNI context silently keeps the default CA. A client holding a certificate trusted by the default CA, but not the protected CA, can therefore complete mTLS to the protected hostname and read its response even with `requestCert` and `rejectUnauthorized` enabled, while a client certified by the protected CA is rejected. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	4.2	More Details
CVE-2026-126839	A deserialization type-restriction control in the BSON serialization component can be bypassed because the check used to recognize a class of compiler-generated types relies on an overly permissive heuristic rather than a precise identification. An unauthorized party able to supply BSON content that an application later deserializes into a loosely typed member can cause types outside the intended allow-list to be constructed and populated with unauthorized party-supplied values inside the consuming application. This can lead to unexpected object state and errors in downstream application logic. No elevated privileges beyond the ability to place unauthorized party-influenced content in the deserialization path are required.	4.2	More Details
CVE-2026-116081	Sleipnir Mobile for iPhone / iPad and Sleipnir Mobile for iPhone / iPad Black Edition provided by Fenrir Inc. are vulnerable to improper certificate verification. A man-in-the-middle attack may allow an attacker to eavesdrop on an encrypted communication.	4.2	More Details
CVE-2026-125870	BookStack before 26.09.3 contains a missing authorization vulnerability in ImageController::checkImagePermission() that allows authenticated non-admin users to bypass page-level content restrictions for images whose owning page has been moved to the recycle bin, because the permission check relies on Page::getPage() which returns null for soft-deleted pages and silently skips the PageView check. Attackers can enumerate sequential image IDs via GET /images/edit/{id} to disclose metadata of restricted images, and users with image-update-all/image-delete-all privileges can rename, replace, or permanently delete images belonging to content they cannot view, persisting the damage even after the page is restored.	4.2	More Details
CVE-2026-110178	IBM ContextForge MCP Gateway 1.0.0 through 1.0.11 is vulnerable to improper access control in the bulk import path. A remote authenticated attacker holding a team-scoped `admin.import` permission can overwrite the endpoint URL, request headers, and authentication credentials of public tools, resources, and prompts owned by other tenants by sending a crafted POST request to `/v1/import` with `conflict_strategy=update`, redirecting subsequent AI gateway invocations to an attacker-controlled host.	4.1	More Details
CVE-2026-110984	The RegistrationMagic WordPress plugin before 6.1.0.4 does not sanitise and escape a parameter before using it in a SQL statement, which could allow high privilege users such as admin to perform SQL injection attacks.	4.1	More Details
CVE-2026-118439	The Limit Login Attempts Security WordPress plugin before 3.4.2 does not validate the destination of a server-side request built from a user-supplied setup value, allowing users with administrator privileges to make the site issue requests to arbitrary hosts, including internal ones (SSRF).	4.1	More Details
	MCUboot's serial-recovery image-upload handler bs_upload() in boot/boot_serial/src/boot_serial.c declares const struct flash_area *fap = NULL and assigns it only via flash_area_open() part-way through the function. Two early validation failures (goto out_invalid_data) — a CBOR map that fails to decode, or an upload packet missing the off/data members — branch past the open while fap is still NULL, then fall into the shared epilogue. In		

CVE-2026-16659	MCUBOOT_ENC_IMAGES builds that epilogue unconditionally calls boot_handle_enc_fw(fap), which reaches boot_image_load_header() and flash_area_read() and dereferences the NULL flash_area. The defect is reachable pre-authentication: the trigger is the very first serial-recovery upload command carrying a malformed payload. The guarding conditions are default-true on a fresh recovery session — img_num, curr_off and img_size are zero-initialized statics, so curr_off == img_size and the primary-slot test both hold. It requires a non-default build: encrypted images (MCUBOOT_ENC_IMAGES / Zephyr CONFIG_BOOT_ENCRYPT_IMAGE) together with an active serial-recovery transport, on the Zephyr or Mynewt port (the two that build both boot/boot_serial/src/boot_serial.c and boot_serial_encryption.c with MCUBOOT_ENC_IMAGES). The impact is a transient denial of service of the bootloader during recovery. fap is a hard NULL rather than an attacker-controlled value, so there is no memory-corruption or information-leak primitive and image authentication is unaffected. Whether the dereference faults is platform-dependent — on targets where address 0x0 is mapped readable flash the read merely returns an error and execution continues, while targets that trap NULL (MPU / null-pointer-exception detection) take a hard fault. Because serial recovery is unauthenticated by design and already permits the console attacker to write the secondary slot, the added capability is only a low-value transient crash. The related unconditional flash_area_close(fap) call in the same epilogue is a safe no-op on the ports that reach it, so it does not contribute to the dereference. The affected ports are the Zephyr port — boot/zephyr/CMakeLists.txt compiles boot_serial.c under CONFIG_MCUBOOT_SERIAL and boot_serial_encryption.c under CONFIG_BOOT_ENCRYPT_IMAGE — and the Mynewt port, whose mcuboot_config.h defines MCUBOOT_SERIAL unconditionally and MCUBOOT_ENC_IMAGES under any BOOTUTIL_ENCRYPT_ syscfg, with boot/boot_serial/pkg.yml declaring no explicit source list so the whole directory is built. The Espressif port is not affected**: it compiles boot_serial.c but not boot_serial_encryption.c, and defines no MCUBOOT_ENC_IMAGES, so the #ifdef MCUBOOT_ENC_IMAGES block containing the call is preprocessed away. The NuttX, Cypress and Mbed ports do not build boot_serial.c at all.	4.0	More Details
CVE-2026-108290	IBM Cyber Fraud 1.0.0 through 1.1.0 could allow an attacker with local access to a container to extract sensitive information due to unrestrictive network policies.	4.0	More Details
CVE-2026-127209	Xiaomi Mi Browser Android Application (com.mi.globalbrowser) before 14.66.0-gn contains a path traversal vulnerability in the exported ThirdDocViewerActivity component, where CopyExternalFile.copyFromUri() copies content provider streams using an unsanitized filename from the _display_name column without basename reduction or canonical-path checks. A zero-permission co-resident malicious application can supply a crafted content provider with a _display_name containing .. sequences to make the browser write attacker-controlled bytes to an arbitrary path within its external storage directory, escaping the intended cache_docs staging location without requiring user interaction.	4.0	More Details
CVE-2026-126644	A link-following flaw was found in the authorized_key module of the ansible.posix collection, residual to the fix for CVE-2026-11837. That fix guards only the final path component (os.chown with follow_symlinks=False and O_NOFOLLOW in _safe_open_write()). When an unprivileged local user replaces their ~/.ssh directory with a symlink to a directory they do not own, and an operator subsequently runs the authorized_key task as root (a common provisioning pattern), the module resolves its path operations through the symlink: atomic_move() writes the temporary file in the symlink target and renames it to <target>/authorized_keys, creating or overwriting a file in the attacker-chosen directory, and os.chmod(sshdir, 0o700) follows the symlink and changes the target directory's permissions. The written file is chowned to the unprivileged user, so this is not a privilege escalation, but it allows an attacker to create or overwrite files (for example in /etc/apt/apt.conf.d/, which APT reads regardless of file ownership) to cause integrity and availability impacts.	3.9	More Details
CVE-2026-126216	A improper privilege management vulnerability in Fortinet FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager Cloud 8.0.0 through 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12 may allow an authenticated administrator to escalate their privileges, bypass authorization controls or impersonate internal services via specially crafted requests to the GUI.	3.8	More Details
CVE-2026-128031	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains an incorrect authorization vulnerability because admin controllers' _isAllowed() checks fall back to, or only check, parent ACL resources instead of finer per-action permissions. Authenticated restricted administrators can mass cancel or hold orders, rewrite order shipping addresses, export customer report data, or create REST roles despite their role denying those permissions.	3.8	More Details
CVE-2026-106468	The Code Snippets WordPress plugin before 4.1.0 does not verify network-level capabilities before honouring a network-scope parameter on its snippet import routes on multisite, allowing an administrator of a single subsite without network-management rights to create, overwrite and deactivate network-wide snippets belonging to the whole network.	3.8	More Details
CVE-2026-120490	On Scalable Platforms, an administrator with permissions to edit and install the Access Control Policy and NAT rules can create a NAT rule that redirects traffic to the Gateway's Sync interface, bypassing the built-in Sync protection. This could allow the administrator to execute operating system commands and write files on the Gateway with superuser privileges.	3.8	More Details
CVE-2026-82175	Dell PowerStore contains a Server-Side Request Forgery (SSRF) vulnerability. A high-privileged attacker could exploit this vulnerability to reach internal network services from the appliance.	3.8	More Details

CVE-2026-110041	The Crop Thumbnails WordPress plugin before 1.10.0 does not perform object-level authorization when reading and re-cropping media attachments, allowing any authenticated user with the upload capability (the Author role by default) to read the metadata of, and overwrite the generated thumbnail files and stored metadata of, media attachments belonging to other users.	3.8	More Details
CVE-2026-124673	The Burst Statistics WordPress plugin before 3.7.5 does not check that a reported page view belongs to published content, nor check post status before listing post titles and links in its public statistics output, allowing unauthenticated attackers to disclose the titles and permalinks of draft, pending and private posts.	3.7	More Details
CVE-2026-129135	picoquic before 2026.11.05.3e2e3d3 contains an integer overflow vulnerability in picoquic_decode_time_stamp_frame() that allows remote QUIC peers to corrupt stored timestamps by sending oversized TIME_STAMP values. Attackers on connections negotiating the TIME_STAMP extension can send large values shifted by ack_delay_exponent to wrap the result, corrupting RTT and bandwidth estimation and degrading congestion control.	3.7	More Details
CVE-2026-128087	russh is a Rust SSH client and server library that includes an SSH agent protocol implementation. From version 0.55.0 until version 0.65.1, the initial key exchange invokes client::Handler::kex_done() with the raw shared secret before check_server_key() accepts the server host key or certificate. A malicious SSH server can therefore trigger application-defined secondary-channel initialization or early data handling even when the server identity is subsequently rejected. Ordinary clients that keep the callback's no-op default or independently defer callback-derived actions until trust is confirmed are not affected. This issue is fixed in version 0.65.1.	3.7	More Details
CVE-2026-126639	The WP Ultimate CSV Importer WordPress plugin before 9.2, WP Ultimate CSV Importer Pro WordPress plugin before 9.0.7 do not protect the files created by their single post export feature, writing them to a publicly accessible location under a predictable name, allowing unauthenticated attackers to download the content and custom fields of any exported post, including non-public content.	3.7	More Details
CVE-2026-63170	Omnispace Agora Project through 26.10.0 contains a predictable token generation vulnerability that allows unauthenticated attackers to forge the shared-calendar iCal share token by deriving md5Id() from predictable fields such as object creation time, which is self-disclosed through autorDate and the iCal CREATED field. Attackers can compute the creation minute and forge the md5Id token to access and read a shared calendar's iCal feed without authorization.	3.7	More Details
CVE-2026-120725	With `REQUIRE_SIGNIN_VIEW = true`, the Git LFS endpoints still answered unauthenticated requests for repositories that are not private. An anonymous client who knows the path of such a repository and the SHA-256 of an LFS object could download the object, and could use the batch endpoint to test whether an object exists. The Git LFS endpoints now require authentication when sign-in is required to view the instance.	3.7	More Details
CVE-2026-126188	Active Storage makes it simple to upload and reference files in cloud services and attach those files to Active Record objects. Prior to 8.0.5.2 and from 8.1 until 8.1.4.1, Active Storage's ActiveStorage::Previewer::VideoPreviewer, ActiveStorage::Analyzer::VideoAnalyzer, and ActiveStorage::Analyzer::AudioAnalyzer pass uploaded blob contents to FFmpeg without restricting the demuxer. A direct upload can retain a client-declared video/* or audio/* content type for an HLS playlist. FFmpeg content probing selects the hls demuxer, which opens attacker-named file:// segments when the blob is previewed or analyzed. Applications that accept untrusted uploads and generate video previews or analyze video or audio attachments can disclose a local media file readable by the application process when the attacker knows its path. This issue is fixed in versions 8.0.5.2 and 8.1.4.1.	3.7	More Details
CVE-2026-76080	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Prior to version 0.224.0, the public Trust Center GraphQL API exposes Query.node(id:) with @authentication(required: OPTIONAL) — an unauthenticated internet visitor to any published trust center can call it. Six of its type branches — Organization, Framework, Audit, ThirdParty (subprocessor), TrustCenter, and TrustCenterReference — resolve the object with a tenant scope derived from the client-supplied GID itself (coredata.NewScopeFromObjectID(id)) and load it with a bare Get(scope, id) that performs no comparison to the current trust center's OrganizationID and no showOnTrustCenter/visibility check. (The Document and File branches, by contrast, correctly pass trustCenter.OrganizationID and check visibility). This issue has been patched in version 0.224.0.	3.7	More Details
CVE-2026-128042	OpenMage magento-lts before 20.19.0 and 21.0.0-beta1 before 21.0.0-beta3 contains a race condition in shopping cart price rule usage limits, because Mage_SalesRule_Model_Validator checks coupon limits without locking and the usage counters are later incremented non-atomically. Unauthenticated attackers, including guest shoppers, can submit concurrent checkouts to redeem a limited coupon more times than its cap allows.	3.7	More Details
CVE-2026-91892	Dell Terraform Provider for PowerFlex, versions prior to 1.9.0, contains a vulnerability that may permit the use of deprecated cryptographic protocols during secure communications. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	3.7	More Details
CVE-2026-126204	express-rate-limit is a basic rate-limiting middleware for Express. From 8.6.0 until 8.7.2, the built-in MemoryStore returns a Client whose mutable resetTime object is retained by middleware using skipFailedRequests or skipSuccessfulRequests. When a later request resets the client window, MemoryStore.resetClient mutates that same Date, so an earlier request that finishes or disconnects after the reset can pass the stale-window guard and decrement the current window's count. A client able to keep requests in flight across the boundary can obtain a bounded extra burst of up to one additional configured limit in the new	3.7	More Details

	window; the behavior does not increase the sustained rate. Stores that return a fresh Date are not affected. This issue is fixed in version 8.7.2.		
CVE-2026-128335	Contao 4.6.0 before 5.3.54, 5.4.0-RC1 before 5.7.17, and 6.0.0-RC1 before 6.0.6 fails to invalidate existing user sessions when two-factor authentication is enabled or disabled. Because Contao\User::isEqualTo() and serialized session data omit two-factor state, attackers already holding a session keep it after the owner changes 2FA settings.	3.7	More Details
CVE-2026-126935	Zipline before 4.8.0 contains a race condition vulnerability in src/server/routes/raw/[id].ts that allows remote attackers to bypass file maxViews limits through non-atomic view counting. Attackers holding a file link can send parallel requests that read the same pre-increment count, viewing view-limited or delete-on-max-views files beyond their limit.	3.7	More Details
CVE-2026-100290	The regcomp and regexec functions in the GNU C Library version 2.3 to version 2.44 may read freed memory and free the same heap block twice when a memory allocation fails while a regular expression is compiled or matched. The re_dfa_add_node (the NFA node table) and build_range_exp (bracket ranges) grow several arrays with consecutive realloc calls and store the new pointers only after all of them succeed. When a later call fails, the pattern buffer keeps pointers to blocks that were already freed, and the error cleanup frees them again. In regexec, the back-reference cache (match_ctx_add_entry) frees its array when a realloc fails but keeps the pointer, which is freed again on the error path. An attacker does not need to supply a crafted regular expression: patterns large enough to grow these arrays are common. The failure has to hit a specific allocation, though, so the issue can only be reached when the system is already under memory pressure. An attacker who supplies the pattern or the subject string has little control over which allocation fails, so the expected impact is a crash of the process. This issue affects all architectures and ABIs supported by the GNU C Library.	3.7	More Details
CVE-2026-110949	The Download Manager WordPress plugin before 3.3.73, Download Manager WordPress plugin before 7.6.2 does not verify a package's configured role restriction when validating a package password, allowing an unauthenticated user who knows the password of a role-restricted package to obtain a download key and download the protected file.	3.7	More Details
CVE-2026-110948	The Download Manager WordPress plugin before 3.3.73, Download Manager WordPress plugin before 7.6.2 does not verify that a visitor is allowed to access a package before its media-preview renderers issue a download key for it, allowing unauthenticated visitors to download password-locked and role-restricted files by reading the key from a public page.	3.7	More Details
CVE-2026-127274	A vulnerability was found in Linksys EA8100 1.0.3.216940. This vulnerability affects unknown code of the file /jnap/core/CheckAdminPassword. The manipulation results in improper restriction of excessive authentication attempts. The attack may be performed from remote. The attack requires a high level of complexity. It is stated that the exploitability is difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2026-128021	FrankenPHP before 1.13.2 contains an information disclosure vulnerability that allows later clients to read earlier clients' libxml errors because worker mode never resets LIBXML(error_list) between requests. Attackers sending requests to the same worker thread can call libxml_get_errors() or libxml_get_last_error() to obtain other clients' parsed-document fragments and server filesystem paths.	3.7	More Details
CVE-2026-128018	FrankenPHP before 1.13.4 contains a denial of service vulnerability in worker mode where frankenphp_handle_request() returns false without finishing the dequeued request after a fatal error during request startup. Attackers who trigger startup fatal errors against worker scripts that keep calling frankenphp_handle_request() can leave client requests hanging indefinitely while the worker continues running.	3.7	More Details
CVE-2026-126406	The wasmtime-wasi-http p2 implementation in Wasmtime before 36.0.20, 37.0.0 before 48.0.8, 49.0.0 before 49.0.5, and 50.0.0 before 50.0.1 can send conflicting content-length headers, or ones not matching the body, in outgoing requests. A guest that reuses a received response's headers resource to send a bodyless request can enable request smuggling against non-compliant servers, potentially bypassing embedder destination access controls.	3.7	More Details
CVE-2026-126400	Password Pusher from 1.49.0 before 2.17.0 contains an IP spoofing vulnerability that allows remote clients to forge the recorded request IP via unanchored trusted-proxy regular expressions. Clients in 110.0.0.0/8 or 210.0.0.0/8, or connecting directly, can supply X-Forwarded-For values to falsify audit log entries and shift password generator rate limits.	3.7	More Details
CVE-2026-16240	Use of externally-controlled format string in PostgreSQL pg_basebackup allows an attacker having already compromised a server to achieve disclosure from pg_basebackup memory, via backup manifest bytes. The vulnerability does not return the improperly-read bytes back to the attacker's server, so a successful attack would need separate implementation-specific secrets for that. Integrity impact is unlikely; in particular, the applicable formatter does not support %n. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	3.7	More Details
CVE-2026-127276	A vulnerability was identified in Linksys EA8100 1.0.3.216940. Impacted is an unknown function of the component Web UI. Such manipulation leads to cookie without 'httponly' flag. It is possible to launch the attack remotely. This attack is characterized by high complexity. The exploitability is considered difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details

CVE-2026-126390	n8n before 1.123.89 contains a credential leakage vulnerability in the NocoDB node that sends the configured NocoDB API token to attacker-chosen hosts when downloading attachments. Attackers with write access to a NocoDB attachment cell can insert a URL to their host, capturing the API token when the workflow executes with Download Attachments enabled.	3.7	More Details
CVE-2026-118410	Exposure of Resource to Wrong Sphere in Apache Roller 4.0 through 6.1.6 allows an unauthenticated visitor to read an entry after its author has withdrawn it to draft through the AtomPub API. The entry was removed from the weblog but stayed in the search index, and public search showed its content. AtomPub is disabled by default. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which shows only published entries in search results.	3.7	More Details
CVE-2026-126388	n8n before 2.46.1 contains a credential exposure vulnerability that forwards Authorization headers and basic auth credentials on cross-origin redirects because sendCredentialsOnCrossOriginRedirect defaults to true. Attackers controlling a redirect target or an expression-fed URL in credential-using nodes can capture stored workflow credentials sent to their endpoint.	3.7	More Details
CVE-2026-128017	FrankenPHP before 1.13.4 contains a double free vulnerability in worker mode that frees SG(request_info).content_type_dup twice when a worker script ends its loop after a non-form POST request. Unauthenticated attackers can send repeated JSON POST requests until the worker loop ends, aborting the whole process when USE_ZEND_ALLOC=0 is set.	3.7	More Details
CVE-2026-122087	The Event Tickets and Registration WordPress plugin before 5.30.3.1 does not restrict attendee data to events the requester is allowed to view, allowing unauthenticated users to retrieve the attendees of private and other non-public events.	3.7	More Details
CVE-2026-129267	A vulnerability was found in sergix44 XBackBone up to 3.8.2. Impacted is the function MediaController::getRawById of the file app/Controllers/MediaController.php. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. The pull request to fix this issue awaits acceptance.	3.5	More Details
CVE-2026-129259	A weakness has been identified in Mereithhh VanBlog up to 0.54.0. This affects an unknown part of the file packages/server/src/types/access/access.ts of the component Image Upload Endpoint. Executing a manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-128051	OpenMage magento-lts before 20.18.2 and 21.0.0-beta1 before 21.0.0-beta3 contains a stored cross-site scripting vulnerability because storefront MSRP/MAP popup and Qty Increments notice templates output product names without proper escaping. Attackers with admin product-edit rights can store a malicious product name that executes script when shoppers view product, category, or wishlist pages.	3.5	More Details
CVE-2026-126814	blueprintUE Self-Hosted Edition before 4.3.6 contains an iframe injection vulnerability that allows authenticated users to embed arbitrary third-party content by abusing the PeerTube video URL matcher in BlueprintService::findVideoProvider(). Attackers can set a blueprint video URL on an attacker-controlled host, which site.js loads in an unsandboxed iframe after consent, framing fake login forms or malware downloads.	3.5	More Details
CVE-2025-15714	The Live Composer WordPress plugin before 2.1.24 does not sanitise and escape some of its Button module settings before outputting them on the front end, which could allow high-privilege users such as administrators to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (e.g. in multisite setups).	3.5	More Details
CVE-2025-15713	The Live Composer WordPress plugin before 2.1.24 does not sanitise and escape some of its page-builder module settings before outputting them, allowing users with access to the builder (Administrator by default) to inject arbitrary JavaScript that executes when the affected page is viewed by any visitor; this has impact even on administrators where the unfiltered_html capability is disallowed, e.g. in multisite setups.	3.5	More Details
CVE-2025-15712	The Live Composer WordPress plugin before 2.1.24 does not sanitise and escape some of its staff member settings before outputting them in pages, which could allow high-privilege users such as administrators to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (e.g. in multisite setups).	3.5	More Details
CVE-2025-15711	The Live Composer WordPress plugin before 2.1.24 does not sanitise and escape some of its module settings before outputting them in an href attribute, which could allow high-privilege users such as administrators to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (e.g. in multisite setups).	3.5	More Details
CVE-2026-61637	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Prior to versions 2.12.7 and 2.13.1, an attacker can craft a URL that, once visited by an authenticated user (or one that is able to authenticate), allows to manipulate the backend to redirect the user to any location. For this to succeed, the victim's locale in Icinga Web must be different from en_US. This issue has been patched in versions 2.12.7 and 2.13.1.	3.5	More Details
	The Widgets for Google Reviews WordPress plugin before 14.3, WP Tripadvisor Review Widgets WordPress plugin before 14.3, Widgets for Booking.com Reviews WordPress plugin before 14.3, Widgets for Reviews &		

CVE-2026-125711	Recommendations WordPress plugin before 14.3, Widgets for Airbnb Reviews WordPress plugin before 14.3, Widgets for Yelp Reviews WordPress plugin before 14.3, Widgets for Amazon Reviews WordPress plugin before 14.3, Widgets for Thumbtack Reviews WordPress plugin before 14.3, Widgets for Ebay Reviews WordPress plugin before 14.3, Widgets for Zillow Reviews WordPress plugin before 14.3, Widgets for Capterra Reviews WordPress plugin before 14.3, Widgets for Expedia Reviews WordPress plugin before 14.3, Widgets for Opentable Reviews WordPress plugin before 14.3, Widgets for WordPress Reviews WordPress plugin before 14.3, Widgets for Hotels.com Reviews WordPress plugin before 14.3, Review Widgets for Szallas.hu WordPress plugin before 14.3, Widgets for AliExpress Reviews WordPress plugin before 14.3, Widgets for Árukereső Reviews WordPress plugin before 14.3, Widgets for Foursquare Reviews WordPress plugin before 14.3, Widgets for Alibaba Reviews WordPress plugin before 14.3, Widgets for SourceForge Reviews WordPress plugin before 14.3 do not sanitise and escape the connected business details before outputting them in their review widgets, which could allow users with the Editor role and above to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in a multisite setup).	3.5	More Details
CVE-2026-126424	OpenEMR before 8.5.0 contains a stored cross-site scripting vulnerability that allows users with admin/superbill write permission to inject HTML into SNOMED code descriptions via superbill_custom_full.php. When a clinician selects the malicious code, the Functional and Cognitive Status form or fee-sheet forms assign it to innerHTML, executing JavaScript in the clinician's session to read patient data and perform actions.	3.5	More Details
CVE-2026-126913	Out of bounds read in Compositing in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.4	More Details
CVE-2026-126359	Hono is a Web application framework that provides support for any JavaScript runtime. From 3.12.0 until 4.13.16, the css helper in hono/css escapes interpolated string values separately and therefore fails to neutralize a closing style tag when < ends the template text or a preceding value and / begins the next attacker-controlled value. During server-side rendering, the combined output can close the <Style /> element early and cause the remainder of the interpolated value to be interpreted as HTML. Applications that place an untrusted string immediately after < in a css template, including adjacent untrusted interpolations, can expose viewers to attacker-controlled HTML or script and information accessible to that page. Other uses of the css helper are not affected. This issue is fixed in version 4.13.16.	3.4	More Details
CVE-2026-119238	A potential improper permissions vulnerability was reported in Lenovo XiangBangbang that could allow a local application to perform unauthorized touch gestures.	3.3	More Details
CVE-2026-126627	Creation of Temporary File With Insecure Permissions vulnerability in Apache XML Graphics FOP. This issue affects Apache XML Graphics FOP: through 2.11. Users are recommended to upgrade to version 2.12, which fixes the issue.	3.3	More Details
CVE-2026-126302	NLTK from 3.9.4 before 3.10.4 contains a symlink following vulnerability in nltk.sem.chat80.sql_query() that bypasses the pathsec data-root sandbox containment check. Attackers who can write into a trusted NLTK data root can plant a symbolic link to read SQLite databases outside the sandbox.	3.3	More Details
CVE-2026-5514	IBM Bob 2.0.3 allows unauthorized extensions to retrieve session tokens via the authentication provider API. The token is exposed in the account identifier field during account enumeration, without requiring explicit user consent. This may allow malicious extensions to access sensitive session information and potentially perform unauthorized actions on behalf of the user.	3.3	More Details
CVE-2026-68549	ClickMigrate is a database migration tool for ClickHouse with automatic SQL migration management and version tracking. Prior to version 1.0.3, a path traversal vulnerability in the revision command allowed a crafted migration name supplied via the -m argument to escape the intended migrations directory. Under specific conditions, an attacker could cause the tool to create a .sql file in an arbitrary location writable by the user executing the command. This issue is only exploitable if an attacker can influence the migration name passed to the revision command, such as through an insecure automation or CI/CD pipeline that forwards untrusted input. This issue has been patched in version 1.0.3.	3.3	More Details
CVE-2026-113408	Path traversal in Git allows writing to arbitrary file via cloning and committing to bad repository	3.3	More Details
CVE-2026-19809	The user-mode system call verifier z_vrfy_charger_get_prop() in drivers/charger/charger_handlers.c declares an uninitialized union charger_propval k_val on the kernel (privileged) stack, passes it to the charger driver back end via z_impl_charger_get_prop(), and then copies the full sizeof(union charger_propval) back into the calling user thread's buffer with k_usermode_to_copy(). That discloses kernel stack contents on two paths: On error. The copy-out ignores the driver's return code. In-tree back ends return an error without writing through the value pointer for properties they do not implement: charger_gpio_get_prop() returns -ENOTSUP unconditionally, and bq24190_get_prop() has a default: return -ENOTSUP; arm that never touches val. The whole union is then stack residue. On success. A back end writes only the one union member the requested property selects (for example sbs_charger.c writes the one-byte val->present for CHARGER_PROP_PRESENT and returns 0), yet the handler still copies the whole union, so every byte beyond that member is uninitialized. The handler is compiled only when CONFIG_USERSPACE=y and is reachable by any user-mode thread that has been granted access to a charger device object. K_SYSCALL_DRIVER_CHARGER() validates only the device object and its API pointer, not the property identifier, so an unprivileged thread can choose prop freely: an unimplemented property forces the	3.3	More Details

	error path, a narrow one the success path, and the call can be repeated at will. Each call discloses up to the size of the union (12 bytes on a 32-bit target, 16 bytes on 64-bit targets where the function-pointer members widen it) of supervisor-stack memory. The bytes are residue of earlier kernel-side frames on the thread's privileged stack and can contain kernel object addresses and saved return addresses, which an unprivileged thread cannot otherwise observe and which help defeat address-layout assumptions when exploiting a separate memory-safety defect. There is no integrity or availability impact. Two commits fix it, and both are needed. 5054384e983c skips the copy-out when the back end reports an error. c31cac727d02 zeroes the union before the driver call, so the bytes copied out on success are driver-written data or zeros. A tree carrying only the first still leaks on every successful call.		
CVE-2026-114467	Out-of-bounds write possible in Git when git-merge(1) used on tag with more than two GPG signatures	3.3	More Details
CVE-2026-126922	Out of bounds read in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-118412	Improper Authentication in Apache Roller 5.1.0 through 6.1.6 allows a user whose account an administrator has disabled to sign in again through OpenID and read unpublished entries. The OpenID sign-in path did not check whether the account was enabled. Only sites that enable the non-default OpenID authentication mode are affected; later major versions do not include OpenID 2.0. Users are recommended to upgrade to Apache Roller 6.1.7 or later.	3.1	More Details
CVE-2026-128072	Nuxt is an open-source web development framework for Vue.js. From @nuxt/webpack-builder 3.0.0 and @nuxt/rspack-builder 3.12.2 until 4.6.4, the development middleware trusts Origin, Referer, or Sec-Fetch-Site when the Host header names the same attacker-controlled hostname. After DNS rebinding changes that hostname to a loopback address, a malicious page opened by a developer can read /_nuxt/*.js client chunks and inline source maps, exposing compiled application source, local filesystem paths, and developer-controlled values embedded in the client bundle. The attacker must know or guess the development-server port and induce the developer to open the malicious page; Chrome 142 and later and other Chromium-based browsers that enforce Local Network Access restrictions prompt before a public page can reach the loopback address. The default Vite builder and production builds are unaffected. This issue is fixed in version 4.6.4.	3.1	More Details
CVE-2026-126882	Information leak in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-118531	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11.1 does not prevent a listing's own author from changing its status from pending to published, allowing users with a Subscriber-level account and above to bypass the administrator's listing moderation and publish their own pending listings.	3.1	More Details
CVE-2026-126907	Uninitialized resource in Media in Google Chrome on on Windows prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to potentially read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-118181	The Duplicate Post WordPress plugin before 1.5.8 does not perform a capability check when saving its global settings, relying only on its own role-access list, which allows users of any role an administrator has given Duplicate Post WordPress plugin before 1.5.8 access to, as low as Subscriber, to overwrite those settings, including the role-access list itself.	3.1	More Details
CVE-2026-128076	Nuxt is an open-source web development framework for Vue.js. From 3.21.6 to before 4.0.0 and from 4.4.6 until 4.6.4, the /__nuxt_island path hash uses ohash serialization that does not escape quotes in string values or delimiters in object keys, allowing different island-prop tuples to produce the same path. For prerendering, substituted content is written into the generated page only if the crawler reaches a colliding URL before rendering the page with the legitimate props. Separately, a CDN or reverse proxy that keys island responses by path alone can be primed with the colliding response. If the substituted prop reaches v-html, innerHTML, or another unsafe HTML sink, the response can execute script in the application origin; otherwise the impact is content substitution. Applications that do not use server components or NuxtIsland, islands without attacker-influenced string props, and responses not cached by path alone are unaffected. This issue is fixed in version 4.6.4.	3.1	More Details
CVE-2026-126198	pgEdge Postgres MCP Server enables SQL queries against PostgreSQL databases through Model Context Protocol compatible clients. Prior to 1.1.0, the bundled clients, including the CLI and web client, decided whether to request write confirmation by checking only for the query_database tool name instead of server-published write annotations. Custom pl-do, pl-func, and writing sql tools therefore ran without confirmation on allow_writes connections, including when a model followed instructions in retrieved content. The affected control is a bundled-client warning rather than a server authorization boundary, and other MCP clients do not inherit that prompt. This issue is fixed in 1.1.0.	3.1	More Details
CVE-2026-	Uninitialized resource in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium	3.1	More Details

126853	security severity: High)		
CVE-2026-126490	OpenEMR before 8.5.0 contains active debug code in interface/fax/fax_view.php that executes passthru("groups") and discloses the web server's Unix group memberships. Authenticated attackers with fax module access can supply a nonexistent jid value to reveal groups such as adm or shadow, aiding privilege escalation planning.	3.1	More Details
CVE-2026-126284	NocoDB from 2026.05.2 before 2026.07.0 contains a server-side request forgery vulnerability that allows Editor-role users to fetch internal URLs because data import reused the webhook internal-network exemption. When NC_ALLOW_LOCAL_HOOKS or NC_WEBHOOK_ALLOW_PRIVATE_NETWORK is set, attackers can request internal services via URLs ending in CSV or spreadsheet extensions and read the responses.	3.1	More Details
CVE-2026-128043	OpenMage magento-lts before 20.19.0 and 21.0.0-beta1 before 21.0.0-beta3 contains a cross-site request forgery vulnerability in PayPal cancel and decline return handlers that trust only the checkout session without verifying the request came from PayPal. Attackers can lure a shopper into a cross-site GET to paypal/standard/cancel to cancel their recent uninvoiced order, void pending authorizations, and restore items to the cart.	3.1	More Details
CVE-2026-128365	Removing a team's review request looked up a review by the negated team ID, which for the team with ID 2 is the ID of the built-in Actions user, and marked the review it found as official. In the organization that owns that team, a user who can change the review requests of a pull request could make an approval left by the Actions user count toward the approvals required by branch protection. Merging still required permission to merge. Removing a team review request no longer changes any review.	3.1	More Details
CVE-2026-126848	Uninitialized resource in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-116303	Missing authorization in PostgreSQL type conversion allows a database user to invoke a cast function despite lacking EXECUTE privilege on that function, via foreign keys, to_json(), and others. A successful attack requires the attacker to search each database for access-restricted cast functions and identify confidentiality impact specific to each function implementation found. There are few or no practical examples of an access-restricted cast function or of a cast function having confidentiality impact. Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected.	3.1	More Details
CVE-2026-126338	Replying to a code review comment accepted a review ID that belongs to a different pull request, through the web form, the API and incoming mail replies. A signed-in user could reply on a pull request they can access with the ID of a review in a repository they cannot read, and the new comment was attached to that review and received the diff context of the commented lines. Replies are now only accepted for a review of the same pull request, and for a pending review only from its author.	3.1	More Details
CVE-2026-126845	Uninitialized resource in GPU in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to potentially read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-126844	Uninitialized resource in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-126347	Tornado is a Python web framework and asynchronous networking library. In versions through 6.6.0, applications using tornado.web.RedirectHandler with URL templates that allow attacker-controlled substitutions to influence the destination can be vulnerable to an open redirect using three or more leading slashes. Differences between Python's URL parsing and browser URL interpretation allow a crafted destination to redirect a user to an attacker-controlled host. The remediation for CVE-2026-116578 in version 6.6.0 did not fully address this case. This issue is fixed in version 6.6.1.	3.1	More Details
CVE-2026-126841	Out of bounds read in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-126894	Out of bounds read in Skia in Google Chrome prior to 157.0.8103.78 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-126349	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.0.0 until 2.9.1, Addressable::IDNA.to_unicode can decode Punycode labels that contain bidirectional controls, zero-width characters, control characters, or other default-ignorable format characters. Addressable::URI#display_uri can consequently show a reordered or visually indistinguishable hostname even though host, normalized_host, and network connections use the original encoded hostname. The pure-Ruby backend accepts the full prohibited set, while the native libidn backend is affected from 2.5.2 for characters added after Unicode 3.2. This issue is fixed in version 2.9.1.	3.1	More Details
CVE-2026-	Parse Server from 9.10.6-alpha.1 before 9.10.8-alpha.1 contains an information disclosure vulnerability that allows clients with write but not read access to learn whether fields are stored on MongoDB. Attackers can send updates with dot notation operations on top-level fields and observe internal server errors versus success	3.1	More Details

126392	responses to infer field existence.		
CVE-2026-76078	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Prior to version 0.224.0, the public Trust Center GraphQL API exposes acceptElectronicSignature and recordSigningEvent, both gated only by @authentication(required: PRESENT) @sessionOnly — any self-provisioned trust center identity can call them. The underlying esign.Service.AcceptSignature and esign.Service.recordEvent build the tenant scope from the client-supplied signatureId GID (coredata.NewScopeFromObjectID(req.SignatureID)) and load the signature by that GID. At no point do they verify that the signature belongs to the caller or that the caller's email matches the signature's SignerEmail. As a result, any authenticated trust-center visitor who possesses another visitor's signature GID can: (1) complete that visitor's NDA signature — overwriting signer name/IP/UA with attacker data and setting status to Accepted, which triggers the sealing worker to generate a completion certificate; (2) inject arbitrary audit-trail events into any signature's log. Both attacks defeat the non-repudiation and integrity guarantees of the e-signature system. This issue has been patched in version 0.224.0.	3.1	More Details
CVE-2026-118408	Missing Authorization in Apache Roller 4.0 through 6.1.6 allows any logged-in user to read unpublished entries of a weblog they have no role in. The entry preview checked that the user was logged in, but not that the user had a role in the weblog being previewed. The attacker must know the weblog name and the entry's link name. Users are recommended to upgrade to Apache Roller 6.1.7 or later, which requires a role in the weblog to preview its entries.	3.1	More Details
CVE-2026-127087	Ryot before 10.5.6 contains an authorization bypass vulnerability that allows authenticated users to revoke other users' access links by supplying an arbitrary accessLinkId. Attackers can obtain access link ids from public share URLs and revoke them without ownership checks, breaking shared access for all link users.	3.1	More Details
CVE-2026-127916	bootutil_img_hash() computes the image digest over ih_hdr_size + ih_img_size + ih_protect_tlv_size bytes, all three taken from the candidate image's header, and reads that span out of the slot without checking that it fits in the flash area. The three sizes are also summed without an overflow check. Nothing earlier on the validation path bounds the whole span either: bootutil_img_validate() compares the image size against bootutil_max_image_size() only after the hash has been computed. The callers bound part of the span, or none of it: On the swap and overwrite upgrade path, boot_validate_slot() first runs the image header check (boot_is_header_valid(), later boot_check_header_valid()). Before MCUboot 2.2.0 that check covered only ih_hdr_size + ih_img_size, so for every image the protected-TLV area (ih_protect_tlv_size, a uint16_t, up to 65535 bytes) was hashed without being bounded. From 2.2.0 the check includes ih_protect_tlv_size, except for a compressed image in the secondary slot when MCUBOOT_DECOMPRESS_IMAGES (CONFIG_BOOT_DECOMPRESSION) is enabled, which leaves the same gap of up to 64 KB. Zephyr's single-slot and firmware loaders (boot/zephyr/single_loader.c, boot/zephyr/firmware_loader.c) read the header with boot_image_load_header(), which bounds ih_hdr_size + ih_img_size against the flash area. Before MCUboot 2.4.0 that bound did not include ih_protect_tlv_size, which leaves the same gap of up to 64 KB. From 2.4.0 these loaders bound the whole span. The serial recovery image-list and image-state handlers (bs_list() and bs_set() in boot/boot_serial/src/boot_serial.c) call bootutil_img_validate() with no header check at all, so on those paths ih_img_size is unbounded as well. The image is hashed before its signature is checked, so anyone who can place an image in a slot (an OTA or SMP update delivered through the application, or serial recovery) reaches this read before authentication. Whether a malformed header produces an actual read beyond the area depends on the flash backend: Backends whose flash_area_read() bounds-checks the request (Zephyr, Espressif, NuttX, Mbed) return an error once the chunked read crosses the end of the area. Validation fails and the image is rejected, with no over-read. With MCUBOOT_HASH_STORAGE_DIRECTLY (Zephyr CONFIG_BOOT_IMG_HASH_DIRECTLY_ON_STORAGE, available from 2.2.0, not enabled by default) the span is hashed through a single direct pointer into memory-mapped flash, with no bounds check. The Cypress PSoC6 port's flash_area_read() (boot/cypress/cy_flash_pal/cy_flash_map.c, from 1.6.0) does not bound the read: its assert()s compare against the area's absolute offset rather than its size, and it copies with memcpy(). The bytes read past the area feed only the digest, which is compared internally and never returned, so nothing is disclosed. The realistic effect is a read fault during image validation: up to 64 KB past the slot on the upgrade path and, before 2.4.0, on the Zephyr loaders, and potentially much further on the serial recovery handlers, which skip the header check. Where validation is repeated at every boot (a pending upgrade, or, before 2.4.0, the single-slot loader checking its image), the fault can recur on each reset and keep the device from booting. The fix makes bootutil_img_hash() add the three sizes with boot_u32_safe_add() and reject an image whose span, including the sector offset used in swap-using-offset mode, does not fit in the flash area, before any of it is hashed. Because the bound is applied where the bytes are read, it covers every caller.	2.9	More Details
CVE-2026-16671	split_image_check() in boot/bootutil/src/loader.c declares a fixed uint8_t loader_hash[32] buffer and passes it as the out_hash out-parameter to bootutil_img_validate(). That routine copies IMAGE_HASH_SIZE bytes into out_hash (memcpy(out_hash, hash, IMAGE_HASH_SIZE) in boot/bootutil/src/image_validate.c), where IMAGE_HASH_SIZE is a compile-time constant of 64 for MCUBOOT_SHA512 or 48 for MCUBOOT_SIGN_EC384/SHA-384 (boot/bootutil/include/bootutil/crypto/sha.h). The buffer tracks SHA-256 (32 bytes) while the copy length tracks the configured algorithm, so the write overruns the buffer by 16 or 32 bytes. The overflow is only present in a non-default configuration: the legacy Mynewt split-image feature must be compiled (split_go()/split_image_check(), i.e. neither MCUBOOT_DIRECT_XIP nor MCUBOOT_RAM_LOAD), the digest must be larger than 32 bytes (MCUBOOT_SHA512 or MCUBOOT_SIGN_EC384), and MCUBOOT_SIGN_PURE must be off. split_go() is a public API with no caller inside MCUboot; it is invoked from a Mynewt application. In the default SHA-256 build there is no overflow. The over-written bytes are the one-way digest of the loader	2.9	More Details

	image and the overflow length is fixed at build time, so the contents are not meaningfully attacker-controlled and the size is not attacker-chosen. The realistic impact is bounded, uncontrolled corruption of the bootloader's stack on the split-boot path, manifesting as instability or failed boot in the affected configuration rather than reliable code execution. The fix is to size loader_hash to IMAGE_HASH_SIZE and pass IMAGE_HASH_SIZE as the matching seed length.		
CVE-2026-117490	The Flatsome WordPress theme before 3.20.13 does not enforce the acting user's publish and post-type restrictions on an AJAX save action, allowing users with a role as low as Contributor to publish their own content and change its post type (for example to a product) without holding the required capabilities.	2.7	More Details
CVE-2026-126328	Insertion of sensitive information into sent data in the user endpoints in Devolutions Server 2026.3.13.0 and earlier allows an authenticated user with delegated user-viewing permissions to obtain users' MFA shared secrets via the user API responses.	2.7	More Details
CVE-2026-117524	The Dynific Addons for Elementor (formerly Anywhere Elementor) WordPress plugin before 1.3.1 does not perform a status or capability check when resolving post identifiers passed to one of its shortcodes, allowing authenticated users with at least the Contributor role to disclose the content of other users' draft, private and password-protected posts. An Author can republish that content to anonymous visitors.	2.7	More Details
CVE-2026-118241	The Smush WordPress plugin before 4.3.6 does not verify that a user is authorised to act on the targeted media attachment, only checking a broad upload-files capability, which allows users with the Author role and above to optimise and restore attachments owned by other users, altering their files on disk and consuming the stored backup.	2.7	More Details
CVE-2026-128052	OpenMage magento-lts before 20.19.0 and 21.0.0-beta1 before 21.0.0-beta3 contains an incorrect authorization vulnerability in the template filter's {{layout}} directive, which renders arbitrary layout handles without enforcing the admin/block whitelist that the {{block}} directive applies. Administrators with rights to edit email, CMS, widget or newsletter content can embed {{layout}} with arbitrary handles to render disallowed blocks and disclose limited information.	2.7	More Details
CVE-2026-115871	The WP STAGING – Backups & Restore, Migration & Clone Plugin – Cloud Backups, Scheduled Backups plugin for WordPress is vulnerable to Arbitrary Directory Deletion in all versions up to, and including, 4.19.0. This is due to insufficient path validation in the `cleanStagingDirectory` function, where the `deleteDir` parameter is only stripped of whitespace and double slashes by `sanitizePath()` without removing `..` traversal sequences or enforcing containment within the staging directory, leaving the sole pre-deletion guard as a simple string equality check against the WordPress home path. This makes it possible for authenticated attackers, with administrator-level access and above, to recursively delete arbitrary directories on the server — including `wp-content`, `wp-admin`, or directories outside the WordPress installation on shared hosting — resulting in denial of service or permanent data loss. An attacker must sequence a clone start, cancellation, and restart to drive the `delete_job` cache into the `directory` step before re-cancelling with a manipulated `deleteDir` value supplied via the `wp_ajax_wpstg_cancel_clone` endpoint.	2.7	More Details
CVE-2026-93333	Vault's audit devices did not validate the contents of a configured audit log prefix and did not consistently enforce the server-level setting that restricts audit log prefixing. This may allow a privileged operator to inject content into audit logs, potentially leading to forged or misleading audit records. This vulnerability (CVE-2026-93333) is fixed in Vault Community Edition 2.2.2 and Vault Enterprise 2.2.2, 1.21.14, and 1.19.25.	2.7	More Details
CVE-2026-126331	Insertion of sensitive information into sent data in the user list endpoint in Devolutions Server 2026.3.13.0 and earlier allows an authenticated user with delegated user-viewing permissions to obtain users' API key secret hashes via the user list API response.	2.7	More Details
CVE-2026-97683	IBM Cyber Fraud 1.0.0 through 1.1.0 could allow a local attacker to bypass security restrictions due to a missing or misconfigured security context.	2.5	More Details
CVE-2026-	boot_save_boot_status() in boot/bootutil/src/boot_record.c reads the image's EXPECTED_HASH_TLV into a stack buffer image_hash[IMAGE_HASH_SIZE] that is never zero-initialised. The TLV handler validates only the upper bound (len > sizeof(image_hash)) and then reads exactly len bytes, so a TLV shorter than IMAGE_HASH_SIZE leaves the tail of image_hash holding stale stack content. The subsequent copy into the boot record, memcpy(buf + offset, image_hash, sizeof(image_hash)), uses the fixed buffer size rather than len, so up to IMAGE_HASH_SIZE - 1 bytes of uninitialised bootloader stack are written into the measured-boot record. The defect is reachable only under MCUBOOT_MEASURED_BOOT, and only when nothing has checked the length of the hash TLV before boot_save_boot_status() reads it. bootutil_img_validate() rejects a hash TLV whose length is not exactly sizeof(hash) (boot/bootutil/src/image_validate.c:345), and primary-slot validation is on by default (Zephyr's CONFIG_BOOT_VALIDATE_SLOT0 defaults to y), so in a default build the malformed image never reaches this code. Two kinds of build let a short TLV through: Builds that use pure signatures (MCUBOOT_SIGN_PURE, Zephyr CONFIG_BOOT_SIGNATURE_TYPE_PURE). The signature covers the image itself, so the hash-TLV check in bootutil_img_validate() is compiled out, and a pure-signed image normally carries no hash TLV. A hash TLV is still allowed in the unprotected TLV area, which the signature does not cover, so a short one can be added to a correctly signed image without invalidating it. This applies with every upgrade strategy, including direct-XIP and RAM-load, and the modified image can be delivered through any path that accepts a signed image. Builds with primary-slot validation turned off: the swap and overwrite loader built without MCUBOOT_VALIDATE_PRIMARY_SLOT, which checks only the image magic before calling	2.4	More

16662	boot_add_shared_data(), and the Zephyr single-slot loader (boot/zephyr/single_loader.c) built without it, including the MCUBOOT_VALIDATE_PRIMARY_SLOT_ONCE variant, which skips validation once the trailer records an earlier successful one. Placing the crafted image requires physical or flash-write access to the device; in a single-slot build with serial recovery enabled, the serial-recovery upload writes the primary slot directly and can place it as well. Outside pure-signature builds, the direct-XIP and RAM-load strategies in boot/bootutil/src/loader.c validate the selected slot unconditionally and are not affected. It is also reachable through a time-of-check/time-of-use change to tamperable external flash between validation and the boot-record read. In these configurations the boot record's measurement is already not trustworthy: the hash copied into the record is the image's own EXPECTED_HASH_TLV, which nothing has verified and which the attacker chooses. The defect therefore does not weaken attestation integrity any further. What it adds is a path for bootloader memory to leave the device: up to 63 bytes (IMAGE_HASH_SIZE - 1) of uninitialised bootloader stack are embedded in the measurement field that a downstream attestation service sends to a remote verifier. In the configurations analysed the residue is bootloader internal state (TLV offsets and lengths, flash addresses, loop state), not key material, but what occupies that stack region depends on configuration and on which code ran before boot_save_boot_status(). It is reported as a low-severity, defense-in-depth disclosure with no integrity or availability impact. This is distinct from the already-fixed record_len integer underflow in the same routine (GHSA-8hrv-4cp5-4rg3). The fix rejects any EXPECTED_HASH_TLV whose length is not exactly IMAGE_HASH_SIZE.		Details
CVE-2026-129251	A vulnerability was detected in hrshadhin CloudSchool up to 3.0.1. This affects an unknown function of the file app/Http/Controllers/Backend/EventController.php of the component Event Description Handler. The manipulation of the argument data results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-129358	A vulnerability was identified in Linux Foundation Magma up to 1.9.0. Impacted is the function handleReact of the file nms/server/main/routes.ts of the component NMS. Such manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-128036	In gittuf 0.4.0 through 0.16.0, when a policy update appears within the range of reference state log entries being verified, verification checks only the root of trust signatures of the new policy and not the signatures of its other metadata (rule files). A user trusted to push to the repository who bypasses gittuf policy apply and writes the policy reference and reference state log directly can make an invalid policy apply during verification, weakening or strengthening the rules for later changes. The update is still recorded in the reference state log.	2.3	More Details
CVE-2026-126316	Frappe HRMS from 16.0.0 before 16.20.1 contains an information exposure vulnerability that places the subscription key in the query string of outbound subscription status requests. Attackers with access to proxy, server, or monitoring logs along the request path can recover the site's subscription key from recorded URLs.	2.2	More Details
CVE-2026-123707	The WPGraphQL WordPress plugin before 2.27.1 does not restrict access to posts in custom non-public post statuses, allowing users with the Contributor role and above to read the content of other users' posts in those statuses.	2.2	More Details
CVE-2026-119033	The Schema & Structured Data for WP & AMP WordPress plugin before 1.70 does not verify that a user may edit a post before letting them change that post's structured data settings, allowing users with the Contributor role and above, when an administrator has granted them access to the Schema & Structured Data for WP & AMP WordPress plugin before 1.70, to disable, alter or reset the structured data of posts they do not own.	2.2	More Details
CVE-2026-128088	russh is a Rust SSH client and server library that includes an SSH agent protocol implementation. Prior to version 0.65.1, try_sign() captures an Arc<PrivateKey> before awaiting Agent::confirm() and does not revalidate the shared lock state or key presence after the await. This is a distinct residual defect in the remediation for CVE-2026-116794. A peer, including a remote SSH server using agent forwarding, can begin a confirmation-constrained signature request while the agent is unlocked and receive the signature after another connection locks the agent if the stale confirmation returns true. New post-lock requests are rejected and private key material is not disclosed, but the pending operation bypasses the current lock state. This issue is fixed in version 0.65.1.	2.2	More Details
CVE-2026-126409	Wasmtime 47.0.0 before 48.0.8, 49.0.0 before 49.0.5, and 50.0.0 before 50.0.1 contains a cross-engine type confusion vulnerability because StructType::with_finality_and_supertype does not validate that the supplied supertype belongs to the same Engine. Embedders using multiple engines that create a GC struct type with another engine's supertype can trigger runtime panics or GC heap corruption, causing denial of service; guest WebAssembly cannot trigger it.	2.0	More Details
CVE-2026-127928	In MCUboot's serial-recovery encrypted-image support (boot/boot_serial/src/boot_serial_encryption.c), decrypt_image_inplace() and boot_image_validate_encrypted() each keep a stack-local struct boot_status. boot_enc_load() writes the plaintext per-image AES key into its enckey[] field. Neither function cleared this structure before returning. In addition, a decrypt failure inside the per-sector loop of decrypt_image_inplace() returned early and skipped the total_out: cleanup, which left the expanded AES key context (enc_data) on the stack as well. The error paths of boot_image_validate_encrypted() similarly skipped boot_enc_zeroize(). The affected code is built when encrypted images (MCUBOOT_ENC_IMAGES, Zephyr CONFIG_BOOT_ENCRYPT_IMAGE) are combined with serial recovery. It runs when an encrypted image is uploaded to the primary slot over the recovery protocol, and when the image list or state is queried while an encrypted image is in the secondary slot. After these functions return, the image's AES content key remains in dead stack memory. An attacker who can	2.0	More Details

	later read device RAM, for example through a debug port or retained RAM, can recover it. This weakens the confidentiality of image-encryption keys within the bootloader trust boundary. A recovered key exposes the plaintext of the encrypted firmware image it protects. The device's long-term private decryption key is not exposed. No remote or recovery-protocol channel that returns this memory is known, so exploitation requires a separate memory-read capability.		
CVE-2026-127915	The MCUboot TLV iterator bootutil_tlv_iter_next() in boot/bootutil/src/tlv.c walks image trailer TLVs with a single loop guard (it->tlv_off < it->tlv_end) and advances by sizeof(struct image_tlv) + tlv.it_len using the attacker-controlled it_len field, without validating that the entry's header or payload stays within it->tlv_end. As a result the 4-byte header read can extend up to 3 bytes past the declared TLV area, and the returned (off, len) can describe a payload that runs past it. The path is pre-authentication: TLVs are parsed during bootutil_img_validate() before the signature is verified, and a crafted image can be presented through DFU / serial-recovery / OTA. However the impact is contained by surrounding guards: bootutil_img_validate() first rejects a TLV area larger than bootutil_max_image_size(), the default LOAD_IMAGE_DATA sink is flash_area_read() which bounds-checks against the flash partition and fails an out-of-partition read, and every payload consumer (EXPECTED_HASH_TLV, EXPECTED_KEY_TLV, EXPECTED_SIG_TLV, IMAGE_TLV_SEC_CNT) clamps len against a fixed buffer before copying. The residual effect in a default flash build is therefore an out-of-region read confined to the attacker's own slot partition whose result is never observable, yielding at worst a clean validation failure rather than memory corruption or information disclosure. A genuine (though still bounded) out-of-bounds read remains under the non-default MCUBOOT_RAM_LOAD configuration, where LOAD_IMAGE_DATA is an unchecked memcpy. The fix is to validate each entry's header and payload against it->tlv_end inside the iterator.	2.0	More Details
CVE-2026-128091	When MCUboot is built with the TinyCrypt crypto backend (MCUBOOT_USE_TINYCRYPT), bootutil_aes_ctr_drop() in boot/bootutil/include/bootutil/crypto/aes_ctr_tinycrypt.h was an empty stub. The AES-CTR context for this backend is the fully expanded AES-128 key schedule (struct tc_aes_key_sched_struct). Generic code relies on this hook to release and clear key state, so with TinyCrypt nothing was cleared. The mbedTLS and PSA backends do free or destroy their key state here. As a result, boot_state_clear(), which boot_go() calls before handing off to the application, left the image's AES content-encryption key schedule in the static boot_data state. This is the case after an encrypted upgrade in single-image builds, where boot_enc_zeroize() is not called. boot_decrypt_key() likewise left the ECIES-derived key-encryption key schedule on the stack. The affected build uses MCUBOOT_ENC_IMAGES with TinyCrypt, which is the default ECDSA and Ed25519 backend in the Zephyr port. The first AES-128 round key equals the cipher key, so anyone who can read the leftover bootloader RAM after boot can recover the image content key and decrypt that encrypted image. That includes a physical attacker with debug or RAM access, or code later running on the device. This weakens image-encryption key confidentiality (and so the confidentiality of the encrypted image's plaintext). The device's long-term private decryption key is not exposed, and image authenticity is not affected. The fix wipes the context with bootutil_wipe_memory().	2.0	More Details
CVE-2026-126408	Wasmtime 47.0.0 before 48.0.8, 49.0.0 before 49.0.5, and 50.0.0 before 50.0.1 contains an insufficient type-check in the TypedFunc embedder API for I31, Option<I31>, and Option<NoneRef> parameter or result types, reaching an unreachable!() path. A malicious guest module exporting a function that uses another anyref-hierarchy type can panic the host embedding, causing denial of service.	1.8	More Details
CVE-2026-114562	OriginLab Origin Viewer OGWU File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGWU files. The issue results from the lack of proper validation of user-supplied data, which can result in a write before the start of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30736.	N/A	More Details
CVE-2026-114556	MailEnable Save Directory Traversal Arbitrary File Creation Vulnerability. This vulnerability allows remote attackers to create arbitrary files on affected installations of MailEnable. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the Save method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of SYSTEM. Was ZDI-CAN-29161.	N/A	More Details
CVE-2026-114561	OriginLab Origin Viewer OPJU File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OPJU files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30433.	N/A	More Details
CVE-2026-114560	OriginLab Origin Viewer OPJ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OPJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30432.	N/A	More Details

CVE-2026-114559	OriginLab Origin Viewer OGG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30431.	N/A	More Details
CVE-2026-114558	OriginLab Origin Viewer OPJU File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OPJU files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30738.	N/A	More Details
CVE-2025-10935	libilbm ILBM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of libilbm. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ILBM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27792.	N/A	More Details
CVE-2026-114563	OriginLab Origin Viewer OGWU File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGWU files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30737.	N/A	More Details
CVE-2026-109094	A integer overflow that can lead to a buffer overrread in the XRes QueryResourceBytes Swap Path in the X.Org xwayland before 24.1.15 and X Server before 21.1.26 on 32bit systems could be used by authenticated clients to crash the X server.	N/A	More Details
CVE-2026-114564	OriginLab Origin Viewer OGG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30768.	N/A	More Details
CVE-2026-8333	A stored cross-site scripting vulnerability in Microchip the TimePictra platform could allow an authenticated, low-privileged attacker to store malicious script content that executes when another user views the affected page	N/A	More Details
CVE-2026-123133	Rejected reason: This CVE ID is a duplicate of CVE-2026-116518 and was never published. Both IDs were assigned to the same vulnerability in the ElasticPress WordPress plugin. All CVE users should reference CVE-2026-116518 instead of this ID.	N/A	More Details
CVE-2026-126991	The Wikidata Lookup expansion module (wiki.py) in MISP misp-modules contained a SPARQL injection vulnerability. The handler function constructed a SPARQL query by directly concatenating the user-supplied text value into the query string without any escaping or parameterization: 'SELECT ?item WHERE { ?item rdfs:label"' + request.get("text") + '" @en }'. An authenticated MISP user with access to the module could supply a crafted text attribute value containing SPARQL syntax (quotes, closing braces, UNION, SERVICE, LIMIT, etc.) to alter the structure of the query sent to the Wikidata SPARQL endpoint. This could allow an attacker to modify the query logic, extract unintended data, or cause the query to fail in ways that expose internal error details. Additionally, the old error handling path formatted raw exception objects into the response string ('wikidata API not accessible {}'.format(e)), potentially leaking internal information such as proxy credentials, query contents, or response bodies. The module also used a spoofed browser user-agent string and the deprecated Wikidata endpoint. The vulnerability required authenticated access to the MISP instance and the ability to invoke the wiki expansion module with a text attribute. The impact is limited to manipulation of the enrichment query and potential disclosure of internal error details; it does not directly compromise the MISP server or its stored data.	N/A	More Details
CVE-2026-47832	The vulnerability lies in the way application credentials are handled within the BOSH deployment. bosh-openstack-cpi-release: all versions from v55 to v55.0.4 (inclusive)	N/A	More Details
CVE-2026-82292	A NULL pointer dereference vulnerability in the Qt Framework QDomDocument::setContent() XML parsing path of the Qt XML module (qtbase).	N/A	More Details
	A vulnerability in the administration REST interface of Azul Payara allows a remote, unauthenticated attacker to		

CVE-2026-110003	bypass secure-admin remote-access restrictions by supplying an arbitrary value in the X-GlassFish-authToken HTTP header. The header's presence waives the remote-rejection check before the token is validated, and an invalid token falls through to password-based authentication, which succeeds without credentials on default domains configured with an empty administrative password. Successful exploitation grants execution of arbitrary administrative commands, equivalent to complete compromise of the server.	N/A	More Details
CVE-2026-90908	A vulnerability in the GenericAdminAuthenticator component of Azul Payara Server and Azul Payara Micro allows a remote, unauthenticated attacker to bypass JMX/RMI administrative access restrictions by spoofing the client host address. Successful exploitation can grant administrative access to the MBean server and lead to remote code execution. Azul Payara Micro is affected only when its JMX connector is enabled.	N/A	More Details
CVE-2026-117474	Rejected reason: This is rejected.	N/A	More Details
CVE-2026-117475	Rejected reason: This is rejected.	N/A	More Details
CVE-2026-117476	Rejected reason: This is rejected.	N/A	More Details
CVE-2026-124617	Rejected reason: 歸類為 JSONCPP Open Source 之問題	N/A	More Details
CVE-2026-127016	The MISP Modules website component exposes external tool management endpoints (add, delete, change status, and change configuration) that did not enforce the optional administrator authentication policy. When ADMIN_PASSWORD was configured in the application environment, the module configuration endpoints correctly required an authenticated administrator session, but the external tools management handlers processed requests from anonymous users without any authorization check. An unauthenticated attacker with network access to the website could add arbitrary external tools, delete existing tools, toggle their active status, and modify their configurations including API keys and ingestion URLs. This inconsistency allowed bypass of the intended access control for the external tools management functionality. The vulnerability is conditional on ADMIN_PASSWORD being set; installations without an admin password intentionally permit open management access by design. The affected component is the external_tools Flask blueprint within the MISP Modules website application.	N/A	More Details
CVE-2026-76173	Blind SQL injection vulnerability in the public endpoint `public/webhook/receiver.php` of the WhatsApp module for Dolibarr 1.9. The phone number value derived from the `data.key.remoteJid` parameter, received via a JSON request, is incorporated into an SQL query without escaping or parameterization. With the WHATSAPP_WEBHOOK_ALLOW option enabled, an unauthenticated remote attacker could manipulate this parameter to alter the query. Exploitation using a timing-based technique could allow an attacker to extract information from the database and cause service disruption.	N/A	More Details
CVE-2026-114369	Resource exhaustion vulnerability in the Qt Framework QWebSocket and QWebSocketServer classes of the Qt WebSockets module	N/A	More Details
CVE-2026-127036	Improper neutralization of CRLF sequences ('CRLF injection') vulnerability in ibi WebFOCUS. This issue affects WebFOCUS: 9.1, from 9.2 through 7, and from 9.3 through 7.	N/A	More Details
CVE-2026-127046	The MISP Modules website component contains an information disclosure vulnerability in the external tools management interface. The /external_tools/list endpoint returned stored API keys (the api_key field) in its JSON response via the ExternalTools model serializer. Additionally, the browser-based edit form pre-populated the API key input field with the stored credential value, exposing it in the DOM. The /external_tools/list endpoint is accessible without authentication (the regression tests verify the response for both authenticated and unauthenticated clients), meaning any network-reachable client could retrieve the API keys for all configured external tools. These keys are used by the server to authenticate submissions to external analysis or enrichment services, so their disclosure allows an attacker to impersonate the MISP instance or directly access those external services. The vulnerability also affected the edit workflow: the change_config endpoint previously required the API key to be present and non-empty on every save, forcing the key to round-trip through the client. The browser JavaScript stored the key in a reactive state object and updated the in-memory tool list with the credential value, further increasing the window of exposure in client-side memory and network traffic. Affected component: the website sub-application of MISP Modules, specifically the external_tools module (serializer in models.py, list endpoint, and the external_tools_index.html template). The impact is limited to confidentiality of the stored API keys; no integrity or availability impact on the MISP Modules website itself is indicated by the patch.	N/A	More Details
CVE-2026-	Improper verification of the source of a communication channel vulnerability in Opera Neon on macOS and Windows allows a malicious browser extension to take control of the browser by sending commands through	N/A	More Details

123139	MCP Hub to the built-in Browser Operator extension. This issue affects Opera Neon MCP Hub extension: 0.0.1.		
CVE-2026-125285	Authentication bypass using an alternate path or channel vulnerability in TIBCO TIBCO Platform’s Self-Hosted Control Plane. This issue affects TIBCO Platform’s Self-Hosted Control Plane: from 1 through 1.21.	N/A	More Details
CVE-2026-118855	Akaunting 3.3.0 contains a stored cross-site scripting vulnerability through invoice import. An authenticated user with invoice-creation permission can import HTML in an invoice status field. When another authenticated user opens that invoice's edit form, Akaunting renders the stored status in a hidden input with raw Blade output, allowing attacker-controlled markup to execute in the victim's Akaunting origin.	N/A	More Details
CVE-2026-8332	A hard-coded root password in Microchip TimePictra platform installation files could allow an attacker with access to those files to obtain privileged credentials	N/A	More Details
CVE-2026-114565	OriginLab Origin Viewer OGG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30769.	N/A	More Details
CVE-2026-8331	An unrestricted upload of files with dangerous type vulnerability in the Microchip TimePictra platform allows functionality not properly constrained by access control lists, potentially resulting in remote code execution.	N/A	More Details
CVE-2026-114566	OriginLab Origin Viewer OGM File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30770.	N/A	More Details
CVE-2026-114567	OriginLab Origin Viewer OGWU File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGWU files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30771.	N/A	More Details
CVE-2026-114568	OriginLab Origin Viewer OPJ File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OPJ files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-31587.	N/A	More Details
CVE-2026-114569	OriginLab Origin Viewer OGWU File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of OriginLab Origin Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OGWU files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30430.	N/A	More Details
CVE-2026-118631	Philips Hue Bridge Pro Argument Injection Restricted File Write Vulnerability. This vulnerability allows local attackers to modify files on affected installations of Philips Hue Bridge Pro. An attacker must first obtain the ability to execute low-privileged code within a container on the target system, in order to exploit this vulnerability. The specific flaw exists within the factory data service, which listens on TCP port 5001 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to modify files in the context of the service account. Was ZDI-CAN-33090.	N/A	More Details
CVE-2026-118632	Philips Hue Bridge Pro SQL Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Philips Hue Bridge Pro. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the HTTP service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-33089.	N/A	More Details
CVE-	Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The		More

2026-121741	specific flaw exists within the parsing of SKP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30421.	N/A	Details
CVE-2026-121742	Ashlar-Vellum Cobalt XE File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28757.	N/A	More Details
CVE-2026-121743	Ashlar-Vellum Cobalt AR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28675.	N/A	More Details
CVE-2026-121744	Ashlar-Vellum Cobalt XE File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28172.	N/A	More Details
CVE-2026-121752	Ashlar-Vellum Cobalt LI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LI files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28447.	N/A	More Details
CVE-2026-121753	Ashlar-Vellum Cobalt XE File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28587.	N/A	More Details
CVE-2026-122044	Philips Hue Bridge Pro Protection Mechanism Failure Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of Philips Hue Bridge Pro. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service, which listens on TCP port 443 by default. The issue results from the failure to apply a protection mechanism. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-33086.	N/A	More Details
CVE-2026-13269	Quest NetVault Backup StnzCreateKey Numeric Truncation Error Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Quest NetVault Backup. Authentication is not required to exploit this vulnerability. The specific flaw exists within the StnzCreateKey function. The issue results from the lack of proper validation of user-supplied data, which can result in a numeric truncation error before allocating a buffer. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-28743.	N/A	More Details
CVE-2026-13270	Quest NetVault Backup nvpmgr Integer Underflow Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Quest NetVault Backup. Authentication is not required to exploit this vulnerability. The specific flaw exists within the nvpmgr service, which listens on UDP port 20031 by default. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before allocating a buffer. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-28744.	N/A	More Details
CVE-2026-117687	Movable Type provided by Six Apart Ltd. contains a code injection vulnerability in its Dynamic Publishing functionality. By sending a specially crafted request that is processed by the Dynamic Publishing, an attacker may be able to execute arbitrary PHP code on the affected product.	N/A	More Details
CVE-2026-101107	An OS command Injection issue exists in Air Terminal 6 provided by SoftBank Corp. Arbitrary commands may be executed with the root privilege by a user who can log in to the web management console of the affected product.	N/A	More Details
CVE-2026-118597	Akaunting 3.3.0 contains a stored cross-site scripting vulnerability in custom invoice payment terms. An authenticated Manager can save a crafted custom payment-term value. When an authorized user opens Invoice Settings for the same company, Akaunting inserts the stored value into a client-side event-handler expression, causing attacker-controlled JavaScript to execute in the victim's authenticated origin.	N/A	More Details
	A remote code execution (RCE) vulnerability in Palo Alto Networks PAN-OS® software on Panorama enables an authenticated administrator with network access to execute arbitrary code with root privileges. The security risk		

CVE-2026-0330	posed by this issue is significantly minimized by restricting access to the management interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . Cloud NGFW, Prisma® Access, and standalone PAN-OS firewalls are not affected by this vulnerability.	N/A	More Details
CVE-2026-129456	In FRRouting, bgpd frees the sub-TLV chain of a Tunnel Encapsulation attribute (type 23) while routes stored by bgpd still point to it, if the attribute is received from a neighbor that has "soft-reconfiguration inbound" configured. A cache added to speed up attribute interning while processing the prefixes of an UPDATE checks whether an interned attribute set may be reused by comparing the parsed attributes with themselves, so the check always succeeds. Interning the parsed attributes for the Adj-RIB-In removes the Tunnel Encapsulation sub-TLVs from them, and the copy that bgpd then interns for the route reuses the cached attribute set, which still holds the sub-TLVs, without taking a reference on them. When the route is later replaced, withdrawn or cleared, for example when the session goes down, the sub-TLV chain is freed while still in use, and bgpd then reads it, decrements a reference count inside it and frees it a second time. In the reporter's build without AddressSanitizer this ended in an assertion failure in bgpd's memory accounting, aborting bgpd and dropping all BGP sessions on the router, and the neighbor can repeat it each time bgpd restarts. Because freed heap memory is written to and freed again, consequences beyond a crash cannot be ruled out. An established BGP session is required, and the attribute does not need to be malformed. bgpd processes attribute 23 from every neighbor, including eBGP neighbors, unless it is explicitly discarded, although RFC 9012 requires it to be filtered on eBGP sessions by default. Neighbors without "soft-reconfiguration inbound" are not affected.	N/A	More Details
CVE-2026-108563	Spreadsheet formula injection in conversion-tracking report exports in Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to submit conversion values that are written as formulas instead of text in an XLS workbook. When a user opens the exported report in a spreadsheet application, attacker-supplied formulas can be evaluated. The confirmed impact is formula execution within the workbook; disclosure of information to the attacker has not been established. The issue is fixed in Revive Adserver 6.0.9 by sanitising conversion values before writing them to the affected XLS report sections.	N/A	More Details
CVE-2026-107662	Blind SQL injection in Revive Adserver 6.0.8 and earlier allows an authenticated manager restricted to one agency to extract arbitrary database values through the banner-zone.php and campaign-zone.php administration pages. Permission checks and database queries obtain identifiers through inconsistent request-input precedence, allowing an authorized numeric identifier to pass validation while a different, attacker-controlled value reaches an SQL query. Extracted data can include password hashes and active session identifiers. Reusing an unexpired administrator session can grant administrative access, allowing modification of configuration and disruption of ad delivery. The issue is fixed in Revive Adserver 6.0.9 by consistently selecting POST values before GET values in both global input registration and common input helpers, and excluding cookies from these helpers. Both commits e301dbbb7 and 0aa9d0124 are required for the complete correction.	N/A	More Details
CVE-2026-108558	A reflected cross-site scripting vulnerability in the conversion-statistics pages of Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in an authenticated user's browser by persuading them to visit a crafted URL. An incorrect ownership check validates the advertiser identifier instead of the supplied website identifier, allowing malicious website input to reach HTML output without appropriate encoding. A related output issue affects the hour parameter. The issue is fixed in Revive Adserver 6.0.9 by validating the correct website identifier and normalising the hour parameter before formatting.	N/A	More Details
CVE-2026-108559	A reflected cross-site scripting vulnerability in the iframe invocation options of Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in an authenticated user's browser by persuading them to visit a crafted URL. When generating invocation tags for an any-size zone, the frame_width and frame_height request parameters are included in HTML attributes without appropriate encoding. The issue is fixed in Revive Adserver 6.0.9 by HTML-encoding the affected values in the invocation-option form fields.	N/A	More Details
CVE-2026-108560	A reflected cross-site scripting vulnerability in updates-history.php in Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in a victim's browser by persuading them to visit a crafted URL. Attacker-controlled values are included in XML command attributes without appropriate encoding, allowing injection of executable XHTML into the response. The preliminary session check omits GET xajax requests, exposing an unauthenticated attack path, while authenticated administrator requests also reach the unsafe output. The issue is fixed in Revive Adserver 6.0.9 by applying the session check to both GET and POST requests and encoding XML command attribute values in both response serializers.	N/A	More Details
CVE-2026-108561	A stored cross-site scripting vulnerability in the report date-selection controls of Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in a victim's browser by persuading them to follow a crafted report URL and complete normal reauthentication. An attacker-controlled period_preset value can be saved in the victim's session and inserted into JavaScript without appropriate encoding. The payload can execute on the initial report view and subsequent report views using the stored defaults. The issue is fixed in Revive Adserver 6.0.9 by applying JSON encoding appropriate for the JavaScript context to date-selection values.	N/A	More Details
CVE-2026-108562	A stored cross-site scripting vulnerability in maintenance-appendcode-check.php in Revive Adserver 6.0.8 and earlier allows an authenticated manager to execute JavaScript in an administrator's browser. A manager can store a malicious tracker name and cause the tracker to appear in the append-code maintenance results. When an administrator opens the affected maintenance page, the tracker name is included in HTML without appropriate encoding. The issue is fixed in Revive Adserver 6.0.9 by HTML-encoding tracker names when	N/A	More Details

	displaying the maintenance results.		
CVE-2026-108564	A reflected cross-site scripting vulnerability in the invocation-tag generation interface of Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in an authenticated user's browser by persuading them to visit a crafted URL. When Direct Selection is enabled, an attacker-controlled banner identifier can be included in HTML form fields without appropriate encoding. Direct Selection is disabled by default. The issue is fixed in Revive Adserver 6.0.9 by HTML-encoding banner identifier values in the invocation-option form fields.	N/A	More Details
CVE-2026-122043	repmgr 4.0.0 through 5.5.0 is affected by an OS command injection vulnerability (CWE-78) in event notifications. When event_notification_command is configured, repmgr substitutes the %a (node name), %c (connection string) and %d (details) placeholders into the command and runs it through the shell. %a and %c are inserted without escaping, and %d escapes only double quotes, so shell command substitution still works inside the quoting the documentation recommends. The node name and connection string come from node records in the repmgr.nodes table. An attacker with the credentials of a non-superuser repmgr database user can write a crafted node record and run OS commands, as the operating system user that runs repmgr or repmgrd (usually postgres), on other cluster nodes that process an event using these placeholders. The %a placeholder of failover_validation_command has the same flaw. Deployments whose repmgr database user is a superuser gain no new capability, because a superuser can already run OS commands, and deployments that do not use these placeholders are not affected. The issue is fixed in repmgr 5.5.1. After upgrading, operators must remove any quotes they placed around these placeholders, because a placeholder left inside double quotes is still open to command injection.	N/A	More Details
CVE-2026-108565	A reflected cross-site scripting vulnerability in the popup invocation options of Revive Adserver 6.0.8 and earlier allows an unauthenticated attacker to execute JavaScript in an authenticated user's browser by persuading them to visit a crafted URL. The top, left, timeout and delay request parameters are included in HTML attributes without appropriate encoding. Exploitation requires an existing popup zone, which can be created through the administrator API but is not offered by the normal zone-creation interface. The issue is fixed in Revive Adserver 6.0.9 by HTML-encoding the affected popup option values.	N/A	More Details
CVE-2026-61619	The OWASP core rule set (CRS) is a set of generic attack detection rules for use with compatible web application firewalls. Prior to versions 3.3.10, 4.25.1, and 4.28.0, regular-expression denial of service (ReDoS) affects a shared regex-assembly include used to build 12 Unix RCE detection rules in CRS v4, and the same ambiguous pattern was present in the manually-assembled regexes in 4 rules in CRS v3.3. With a single, unauthenticated, crafted request, the generated pattern drives PCRE2 past its backtracking limit. When PCRE2 exceeds that limit, the @rx operator returns an error rather than a match result, which results in detection bypass and CPU denial of service. This issue has been patched in versions 3.3.10, 4.25.1, and 4.28.0.	N/A	More Details
CVE-2026-65820	aeon is a scikit-learn compatible Python library for learning from time series. Prior to version 1.5.0, a GitHub Actions workflow used pull_request_target for pre-commit checks on pull requests from forks. In this configuration, fork-controlled code could be checked out and executed in a privileged context. The vulnerable workflow also generated/used elevated credentials and could automatically commit or push fixes back to pull request branches. This created a potential token exposure and repository write path if an attacker submitted a malicious fork pull request designed to execute during the privileged workflow run. This issue has been patched in version 1.5.0.	N/A	More Details
CVE-2026-68485	An authorization bypass in website-index.php in Revive Adserver 6.0.8 and earlier allows an authenticated manager restricted to one agency to view another agency's website listing by changing the agencyid request parameter. Disclosed information includes website names, identifiers and timestamps. Detailed website pages continue to enforce ownership checks. The issue is fixed in Revive Adserver 6.0.9 by obtaining the agency identifier from the authenticated account rather than the request.	N/A	More Details
CVE-2026-68486	An authorization bypass in campaign-zone linking in Revive Adserver 6.0.8 and earlier allows an authenticated manager, or a trafficker with zone-linking permissions, to associate another agency's campaign with their own zone. Campaign ownership checks are missing from the bulk-linking and single-link operations in zone-include.php and the XML-RPC campaign-linking method. Although agency filtering prevents foreign banners from being linked, the unauthorized association can expose the foreign campaign's name, type and identifier in the linked-campaign listing. The issue is fixed in Revive Adserver 6.0.9 by validating campaign ownership in the affected operations.	N/A	More Details
CVE-2026-77168	A cross-site request forgery vulnerability in tracker-invocation.php in Revive Adserver 6.0.8 and earlier allows an attacker to modify a tracker's name, description or advertiser assignment using an authenticated victim's permissions. A leftover state-changing handler accepts request parameters without verifying a CSRF token, although it is not used by the normal invocation-tag interface. Exploitation requires victim interaction and a request path that carries the victim's session credentials. The issue is fixed in Revive Adserver 6.0.9 by removing the unused tracker-modification handler.	N/A	More Details
CVE-2026-107247	An authorization bypass in Revive Adserver 6.0.0 through 6.0.8 allows an authenticated manager restricted to one agency to access or modify resources belonging to another agency. Global input registration gives GET parameters precedence over POST parameters, while submitted administration forms use POST values. By supplying authorized object identifiers in the query string and different identifiers in the POST body, an attacker can cause permission checks and subsequent operations to target different objects. This permits unauthorized cross-agency changes, campaign ownership reassignment and disclosure of campaign and banner data. The	N/A	More Details

	regression was introduced in commit 156dee7bc3283c128f35e5a31bb305054cc8de1b and is fixed in Revive Adserver 6.0.9 by restoring POST precedence in global input registration.		
CVE-2026-48479	Use of uninitialized or invalid state in AMD Graphics Driver could allow a local attacker to write out of bounds, potentially resulting in loss of integrity or denial of service.	N/A	More Details
CVE-2026-119055	CWE- 416: Use After Free vulnerability exists that could cause arbitrary code execution when a local attacker could trick the end user to open a specially crafted malicious SSD file.	N/A	More Details
CVE-2026-61810	libspdm is a sample implementation that follows the DMTF SPDM specifications. In version 1.4.0, both the FINISH request (Table 80) and the FINISH_RSP response (Table 81) gained two new fields, OpaqueDataLength and OpaqueData, placed before the trailing signed/authenticated field. The transcript definitions used to compute and verify the FINISH signature, the FINISH HMAC (RequesterVerifyData), and the FINISH_RSP HMAC (ResponderVerifyData) were not updated and still terminate with a step of the form. Per DSP0274, the "SPDM Header Fields" are only the four header bytes (SPDMVersion, RequestResponseCode, Param1, Param2). A literal reading therefore excludes OpaqueDataLength and OpaqueData, even though those fields are transmitted before the trailing signature/HMAC field. Because the signature/HMAC must cover every field transmitted before it to "protect the entire handshake against manipulation by an active attacker," an active attacker could otherwise modify the opaque data in flight without invalidating the signature or HMAC. This issue has been patched in version 1.4.1.	N/A	More Details
CVE-2026-116645	LimeSurvey Community Edition 7.8.0 contains an SQL injection vulnerability in the survey-archive participant import and SPSS-response export workflow. An authenticated user with global surveys.create permission can import a crafted .lsa archive whose participant XML creates an attacker-named attribute column. When the user exports responses from the imported non-anonymous survey, LimeSurvey passes the persisted name to Yii's select builder. Names containing parentheses are treated as SQL expressions instead of quoted identifiers, causing attacker-controlled SQL to execute with the application's database privileges.	N/A	More Details
CVE-2026-63192	OpenMRS module bahmnicore contains Core OpenMRS modules for Bahmni (including ERP & ELIS Atom Feed Clients). In version 0.93, an attacker with authenticated access could potentially exfiltrate sensitive data from the database. This issue has been patched in version 0.93.1.	N/A	More Details
CVE-2026-63194	OpenMRS module bahmnicore contains Core OpenMRS modules for Bahmni (including ERP & ELIS Atom Feed Clients). In version 0.93, there is insufficient validation of input paths during the admin CSV import process, allowing for potential arbitrary file write. This issue has been patched in version 0.93.1.	N/A	More Details
CVE-2026-118368	Akaunting 3.3.0 contains a stored cross-site scripting vulnerability in the XLSX item-import workflow. An authenticated Manager can import an item whose name contains HTML. When another authenticated user selects that item while creating a document, Akaunting places the stored name in an invoice or bill line item through Vue v-html, causing attacker-controlled markup to execute in the victim's Akaunting origin.	N/A	More Details
CVE-2026-59191	TwigView plugin for CakePHP provides wrappers for common View operations and extensions that expose CakePHP functions and jasny/twig-extensions helpers. Prior to versions 1.3.3 and 2.1.2, if FileLoader::findTemplate() is supplied un-validated user controlled data, arbitrary files can be read. This issue has been patched in versions 1.3.3 and 2.1.2.	N/A	More Details
CVE-2026-59192	TwigView plugin for CakePHP provides wrappers for common View operations and extensions that expose CakePHP functions and jasny/twig-extensions helpers. Prior to versions 1.3.3 and 2.1.2, the unserialize filter has no restriction on which classes are allowed. This can used as a deserialization remote-code-execution gadget. This issue has been patched in versions 1.3.3 and 2.1.2.	N/A	More Details
CVE-2026-96414	In affected versions of Octopus Server, insufficient integrity protection of authentication cookies, combined with incorrect validation of permissions assigned to a user that allowed them to view users or audit events, could result in the user escalating their privileges to those of an Administrator.	N/A	More Details
CVE-2026-0470	Null pointer dereference in AMD Embedded SPI Flash driver could allow a local user to potentially cause a loss of availability.	N/A	More Details
CVE-2026-105948	In affected versions of Octopus Server, incorrect validation of permissions assigned to a user that would allow them to edit their own login identities could result in that user being granted elevated permissions, up to and including system administrator access. This issue affects instances using LDAP authentication with self-service login editing enabled.	N/A	More Details
CVE-2026-93487	In affected versions of Octopus Server, incorrect validation of the permissions assigned to a user that would allow them to create project triggers could result in the user being able to run runbooks or create deployments they were not authorised to perform.	N/A	More Details
CVE-2026-	Local privilege escalation vulnerability in Iperius Backup 8.8.3, due to insufficient separation between the graphical user interface running with elevated privileges and local users with low privileges. When the backup service is configured to run persistently with Administrator privileges, a local attacker with low privileges can use the native Windows dialogues exposed by the application to run programmes that inherit its elevated context.	N/A	More Details

112174	This allows commands to be executed with SYSTEM or Administrator privileges, depending on the application’s context, and compromises the affected Windows system.		
CVE-2026-118965	Path traversal in the discovered host label synchronization in Checkmk <2.5.0p19, <2.4.0p40 and 2.3.0 (EOL) allows an attacker in control of a remote site in a distributed monitoring setup to write arbitrary files on the central site and thereby execute code as the central site user.	N/A	More Details
CVE-2026-120495	Path traversal in the Synthetic Monitoring "Robotmk" test service of Checkmk <2.5.0p19, <2.4.0p40, and 2.3.0 (EOL) allows an attacker who controls the agent output of a monitored host's check output for a host to inject a crafted robot output to define the contents and location for the generated HTML log, leading to code execution as the site user.	N/A	More Details
CVE-2026-121374	Argument injection in the Kubernetes special agent in Checkmk <2.5.0p19, <2.4.0p40, and 2.3.0 (EOL) allows a user with permission to edit rules in at least one folder to write files to arbitrary locations writable by the site user via crafted node roles in the "Exclude nodes based on their role" rule option, leading to code execution as the site user.	N/A	More Details
CVE-2026-82978	An authorization bypass in channel-edit.php in Revive Adserver 6.0.8 and earlier allows an authenticated manager to create a delivery rule set belonging to another agency by changing the submitted agencyid parameter. The server trusts the submitted agency identifier when inserting the new rule set, allowing unauthorized creation of objects in another agency's account. The issue is fixed in Revive Adserver 6.0.9 by obtaining the agency identifier from the authenticated account rather than submitted form data and removing the agency identifier from the form's hidden fields.	N/A	More Details
CVE-2026-123828	A one-byte heap buffer overflow in Node.js HTTP/2 Alt-Svc handling lets a remote, unauthenticated attacker corrupt process memory. When an application passes an attacker-controlled value such as a request's :authority header to Http2Session.altsvc(), the AltSvc implementation in src/node_http2.cc allocates a buffer sized to the origin length and then writes it with a null terminator, placing one byte past the end of the allocation. A single request carrying a long but syntactically valid :authority triggers the out-of-bounds write, which aborts the process and serves as a remote heap-corruption primitive. This vulnerability affects Node.js 26.x and 24.x.	N/A	More Details
CVE-2026-107922	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-103980	ideon is a self-hosted visual workspace. Prior to version 0.9.6, the SSRF protection in safeFetch is bypassed by IPv6 transition addresses that embed private IPv4 addresses. The isPrivateIP function in src/app/lib/ssrf.ts checks only a narrow set of IPv6 ranges (loopback ::1, ULA fc/fd, link-local fe80) but does not recognize IPv4-mapped (::ffff:), NAT64 well-known (64:ff9b::/96, RFC 6052), NAT64 local-use (64:ff9b:1::/48, RFC 8215), 6to4 (2002::/16, RFC 3056), or Teredo (2001::/32, RFC 4380) encodings. An authenticated user can supply these addresses in link URLs to reach cloud metadata endpoints (169.254.169.254), localhost services, and RFC 1918 internal networks through the link preview metadata fetcher. This issue has been patched in version 0.9.6.	N/A	More Details
CVE-2026-0326	A buffer overflow vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to disrupt service processing by causing a service process crash or memory corruption. Panorama and Prisma® Access are not affected by this vulnerability.	N/A	More Details
CVE-2026-0327	A privilege escalation vulnerability in the GlobalProtect gateway of Palo Alto Networks PAN-OS® software enables an authenticated, lower-privileged user to obtain the privileges and configuration of a higher-privileged user. Cloud NGFW and Panorama are not affected by this vulnerability.	N/A	More Details
CVE-2026-0328	Authentication bypass vulnerabilities in the GlobalProtect™ portal and gateway of Palo Alto Networks PAN-OS® software enables an unauthenticated user to bypass security restrictions and establish an unauthorized VPN connection. Panorama, Cloud NGFW, and Prisma® Access are not affected by this vulnerability.	N/A	More Details
CVE-2026-0329	A buffer overflow vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to cause a denial of service (DoS) condition by sending specially crafted network traffic to or through a dataplane interface. Cloud NGFW and Panorama are not affected by this vulnerability.	N/A	More Details
CVE-2026-120869	An unauthenticated attacker can bypass authentication controls to access restricted resources on the Citrix NetScaler Console appliance	N/A	More Details
CVE-2026-0331	An information disclosure vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated remote attacker with network access to obtain sensitive firewall and session information by sending traffic to or through a dataplane interface. Panorama is not affected by this vulnerability.	N/A	More Details
CVE-2026-65957	Helio is an MCP proxy that sits between AI agents and the tools they use. Prior to version 0.8.0, the dashboard sideband (default 127.0.0.1:3100) validated CORS request origins by matching the hostname against a private-network string prefix (10., 172.16.–172.31., 192.168.) rather than validating an IP address. A public DNS name such as 192.168.attacker.com, 10.evil.io, or 172.16.pwn.example also satisfies that prefix, so the proxy echoed the attacker origin in Access-Control-Allow-Origin. This issue has been patched in version 0.8.0.	N/A	More Details
CVE-	An incorrect privilege management vulnerability in the OPSWAT MetaDefender Endpoint Security SDK used by		More

2026-0324	the Palo Alto Networks GlobalProtect™ app on Windows devices allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY\SYSTEM.	N/A	Details
CVE-2026-65965	ideon is a self-hosted visual workspace. Prior to version 0.9.4, several project mutation endpoints under /api/projects/[id]/* resolve the caller's project role but never enforce it, so a user who was granted only the read-only viewer role on a project can perform write operations on that project. The most severe is POST /api/projects/[id]/graph, which deletes every block and link in the project and re-inserts client-supplied ones. A viewer can silently rewrite or wipe the entire canvas of a project they were invited to read. The application clearly intends viewer to be read-only: the collaborators endpoint, the automation endpoints, and the realtime Yjs sync path all reject write attempts from viewers. These specific HTTP handlers simply omit the guard their siblings enforce. This issue has been patched in version 0.9.4.	N/A	More Details
CVE-2026-65968	ideon is a self-hosted visual workspace. Prior to version 0.9.4, validateUrlForSSRF() / safeFetch() in lib/oauth/ssrf-protection.ts (and the parallel validateMcpUrl() in lib/security/validators.ts) perform SSRF host-blocking by string/regex matching on new URL(url).hostname. Their IPv6 branch only recognises the textual forms ::1, fe80:/fc00:/fd00: prefixes, and the dotted-decimal IPv4-mapped form ::ffff:127.x. It does not recognise the WHATWG-canonical IPv4-mapped-IPv6 host that Node emits for a mapped address, which is hex-compressed and bracket-wrapped: [::ffff:7f00:1] for 127.0.0.1, [::ffff:a9fe:a9fe] for 169.254.169.254. An authenticated user who registers a STREAMABLE_HTTP / SSE MCP server with URL http://[::ffff:7f00:1]:PORT/ (loopback) or http://[::ffff:a9fe:a9fe]/ (cloud metadata) passes both guards, and the server-side OAuth-discovery action then fetches that host, yielding server-side request forgery to loopback and to the cloud metadata service. This issue has been patched in version 0.9.4.	N/A	More Details
CVE-2026-65982	nginx-http-flv-module is a media streaming server based on nginx-rtmp-module. Prior to version 1.2.14, if a server received an HTTP/1.0 request without a header Host, which was permitted by HTTP core of Nginx, then r->headers_in.host was NULL, nginx-http-flv-module used r->headers_in.host->value to make a pseudo tcUrl, so NULL-pointer dereference happened. This issue has been patched in version 1.2.14.	N/A	More Details
CVE-2026-68507	ideon is a self-hosted visual workspace. Prior to version 0.9.5, ideon's link-preview endpoint requires no authentication at all and forwards any URL a caller supplies straight into a server-side fetch. The app does have a general-purpose SSRF guard (safeFetch/validateSafeUrl in src/app/lib/ssrf.ts), but this route sits behind no login check whatsoever, making it a fully open, anonymous URL-fetch relay - and the guard's IP blocklist itself has a gap that lets it reach the server's own loopback interface via the 0.0.0.0 "any address" bypass, a well-documented SSRF-filter evasion technique on Linux. This issue has been patched in version 0.9.5.	N/A	More Details
CVE-2026-68511	Paaster is a pastebin application. Prior to version 3.3.0, Paaster's "view once" (burn-after-reading) paste mode can be bypassed with concurrent requests. The check that's supposed to enforce single-use is a plain read followed by a separate write, with no atomicity, so multiple simultaneous requests can all see the paste as "not yet read" and all successfully retrieve it. This issue has been patched in version 3.3.0.	N/A	More Details
CVE-2026-68512	Paaster is a pastebin application. Prior to version 3.3.0, Paaster's account login has no rate limiting, lockout, or CAPTCHA of any kind, and a companion endpoint openly discloses whether a username exists along with that account's password-hashing salts. Together these let an attacker enumerate real accounts and then brute-force their passwords with unlimited, unthrottled attempts. This issue has been patched in version 3.3.0.	N/A	More Details
CVE-2026-0325	An authorization bypass vulnerability in the GlobalProtect gateway of Palo Alto Networks PAN-OS® software enables an authenticated attacker with valid GlobalProtect credentials to bypass IP address restrictions and circumvent network access controls that rely on source IP filtering. Cloud NGFW is not affected by this vulnerability.	N/A	More Details
CVE-2026-129349	When authentication caching is enabled on DefaultLdapRealm, after a user logs in successfully once, subsequent logins for that user succeed with any password. A cached authentication skips the LDAP bind, and the AllowAllCredentialsMatcher installed by default in DefaultLdapRealm accepts any credentials, allowing an attacker who knows a valid username to authenticate as that user. This issue affects all Apache Shiro versions through 3.0.0, only when using DefaultLdapRealm (or JndiLdapRealm) with authenticationCachingEnabled set to true, which is not the default. Mitigation: Upgrade to version 3.0.1 or later, which fixes the issue by no longer installing AllowAllCredentialsMatcher by default. Alternatively, disable authentication caching on the LDAP realm (this is the default), or configure a credentials matcher, such as SimpleCredentialsMatcher, that verifies credentials against the cached authentication info.	N/A	More Details
CVE-2026-123829	A Permission Model bypass in Node.js recursive file watching discloses the names of files and directories the process is not permitted to read. On macOS and Windows, fs.watch() and fs.promises.watch() in recursive mode are backed by the native libuv watcher: FSEventWrap::Start checks kFileSystemRead only once, on the watched root, and FSEventWrap::OnEvent then forwards every filename libuv reports (relative paths at any depth) to the JavaScript callback without checking that each path is covered by the read grant. Code running under --permission with an exact read grant on a directory can therefore learn names such as sub/secret.txt even though readdir on that subdirectory is denied. The flaw exposes names and timing metadata, not file contents, and requires macOS or Windows plus files created under the watched directory by another actor. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-	Node.js discloses proxy credentials in ERR_PROXY_INVALID_CONFIG error messages. CVE-2026-48615 established that a proxy credential must not appear in a Node.js error message and redacted the username and password from ProxyConfig.href, but that fix missed four error paths in the same subsystem, one of them inside		

2026-123871	the same constructor, which interpolate the raw proxy URL, credentials included, into an ERR_PROXY_INVALID_CONFIG message. The proxy URL comes from the environment, but the defect is the sink: a secret that Node.js redacts everywhere else is emitted verbatim into a much wider audience than the process environment, such as stderr, container logs, log aggregation, and crash reporting services. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123862	An uncatchable exception in the Node.js zlib streaming API lets a peer crash a process by disconnecting while data is being compressed. zlib.params() queues a flush and completes its work in that write's callback; if the stream is destroyed first, as pipeline() does when the peer goes away, Writable still invokes the callback with an error, but the callback ignores its arguments and asserts that the native handle still exists. The handle is gone, so an ERR_INTERNAL_ASSERTION is thrown from inside stream internals and bypasses the stream's error event, the params() callback, and the pipeline() callback, terminating the process. An application is affected only if it calls deflate.params() while streaming to a peer, which is uncommon. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123863	A reachable assertion in Node.js HTTP/2 session teardown lets any unauthenticated client abort the server, over both TLS and cleartext. A client can arrange for an Http2Stream that still holds nghttp2-allocated header buffers to outlive its session: the stream is removed from the session's stream set but never detached, so when ~Http2Session() runs the memory accounting is nonzero and the CHECK_EQ(current_nghttp2_memory_, 0) assertion fails, terminating the process. The trigger needs only a default http2 server whose handler responds before the request body has ended, which is typical. It is a variant of CVE-2024-27983 that the earlier fix did not cover, because that fix only detached streams still tracked in the session. This vulnerability affects Node.js 26.x (since 26.9.0) and 24.x (since 24.22.0).	N/A	More Details
CVE-2026-123864	A re-entrancy flaw in Node.js HTTPS lets an unauthenticated client read memory belonging to other connections, including TLS private keys and other users' requests. TLSWrap::DoWrite() calls ClearOut() directly when asked to write zero bytes; if that write is issued from JavaScript running inside the HTTP parser's on_body callback, ClearOut() decrypts the next TLS record while the parser is still mid-body, re-entering llhttp_execute() and causing a use-after-free and an out-of-bounds heap read. The server then copies that freed or unrelated heap memory into the response for the request body. Triggering it requires a handler that calls res.flushHeaders() before the request body ends and later calls res.end() with a non-empty chunk, and reading the leaked memory requires any ordinary route that echoes or stores a request body. Cleartext node:http is not affected. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123865	An unauthenticated HTTP/2 client can permanently leak Node.js server memory and file descriptors. If a peer triggers a protocol error, for example an oversized frame header, while the session is already shutting down, nghttp2 tears the session down internally but Node.js never notices, leaving a dangling session: the socket stays in CLOSE_WAIT and all of Node.js's HTTP/2 state for that connection is held in memory indefinitely, with no further cost to the attacker. The attacker can start the shutdown remotely by sending GOAWAY(NO_ERROR), so it is reliable against default HTTP/2 servers. It is an incomplete-fix case of CVE-2026-48937: that fix detected nghttp2 internal terminations by watching for GOAWAY sent while not shutting down, but missed terminations that arrive while the session is already shutting down. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123866	A use-after-free in Node.js HTTP/2 stream teardown can leak response memory, including the contents of other connections' response buffers, to a peer. When a stream is torn down while a write is still backpressured, for example by a peer RST_STREAM or by the server's own per-stream timeout destroying the stream, the stream's response buffer is freed but a reference to it is still used, so freed or unrelated heap memory is written to the socket instead of the intended response. On Node.js 26.x and 24.x the teardown can be driven purely by a remote peer once the window-size change from 26.9.0 and 24.22.0 is present, and on all supported lines the same defect is reachable through an application-initiated teardown such as a per-stream idle timeout. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123868	An unauthenticated HTTP/2 client can exhaust Node.js server memory because inbound DATA queued on an undrained stream is charged to no session budget. Each inbound DATA frame creates one JavaScript Buffer view in the receiving stream's readable queue, but nothing charges that queue to current_session_memory_: the socket read buffer is accounted only during parsing and released immediately, so whatever stays queued is accounted to nothing. A peer that fills a stream's receive window with one-byte DATA frames pays about 10 wire bytes per frame while the server retains about 114 bytes per frame, so a single stream on one connection can retain hundreds of megabytes from tens of megabytes sent. maxSessionMemory neither bounds the growth nor refuses new streams, because Http2Session::CanAddStream gates admission on the same counter that never sees the queue. This vulnerability affects Node.js 26.x and 24.x.	N/A	More Details
CVE-2026-123872	A client certificate authentication bypass in Node.js TLS lets a client change the servername during TLS 1.2 renegotiation to reach endpoints it was not authorized for. On a server that applies different client-certificate policies per hostname, for example stricter admin-only client-cert auth on one host and ordinary client-cert auth on another, a client that authenticates for a permitted host can renegotiate the TLS 1.2 connection under a different servername and carry its existing authentication to the protected host, bypassing the stricter policy. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-0323	A server-side request forgery vulnerability in Palo Alto Networks Checkov by Prisma® Cloud enables a local unauthenticated user to make unauthorized network requests from host to internal services.	N/A	More Details

CVE-2026-123874	A use-after-free in Node.js HTTP/2 lets an unauthenticated client corrupt server memory, over both TLS and cleartext, when the server serves files with respondWithFile() or respondWithFD(). A client can make the server free an Http2Stream while a write request that points to it is still queued on the socket; when that write completes, the code dereferences and makes a virtual call through the freed object. The only precondition is that the application serves a file with stream.respondWithFile() or stream.respondWithFD(), with default settings otherwise. This vulnerability affects Node.js 26.x (since 26.9.0) and 24.x (since 24.22.0).	N/A	More Details
CVE-2026-123875	A NULL pointer dereference in Node.js HTTP/2 lets an unauthenticated client crash the server, over both TLS and cleartext, by cancelling file downloads. When the server serves a file with stream.respondWithFile() or stream.respondWithFD() and the client cancels the request, a StreamPipe used for the transfer is torn down in an order that leaves a NULL pointer which is then dereferenced, aborting the process. No crafted frames are needed, and a handful of cancelled requests against a default file-serving handler is enough. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-123877	A certificate validation bypass in Node.js https.Agent lets a cached TLS session authenticated under one CA policy be reused by a later request with a stricter policy. https.Agent.prototype.getName() assigns the same Agent and session-cache key to a request that omits ca and one that explicitly supplies ca: [], because an omitted value appends nothing to the key while an empty array stringifies to an empty string. The two policies differ: omitting ca uses the default trust store, while supplying ca replaces it. Since they share a key, a TLS session authenticated under the broader default policy is handed to a new connection made under the later ca: [] policy, and TLS 1.3 session resumption carries the earlier authentication forward, so the second request reports authorized === true and transmits confidential data to a server its own CA policy would reject on a fresh connection. This vulnerability affects Node.js 26.x, 24.x, and 22.x.	N/A	More Details
CVE-2026-126051	A deferred-callback use-after-destroy in Node.js TLS server handshake handling allows a remote, unauthenticated attacker to terminate the server process. When a TLS server uses any of the SNICallback, OCSPRequest, newSession, or resumeSession hooks, or server.addContext(), the corresponding OpenSSL callbacks are deferred, and the deferred code does not handle the underlying socket being destroyed between scheduling and execution. By sending a client hello that reaches the vulnerable path (for example, no SNI together with an OCSP request) followed by padding and a socket FIN, an attacker makes OpenSSL deliver the client hello and the end-of-file in the same tick, so the socket is destroyed before the deferred callback runs and the process raises an uncaught exception instead of emitting an 'error' event. This vulnerability affects Node.js 26.x and 24.x.	N/A	More Details
CVE-2026-65833	iopress is a native HTTP server for Node.js with platform-specific async I/O. Prior to version 1.0.5, the chunked-transfer-encoding HTTP request parser in @iopress/core reads past the end of the input buffer when a request declares a chunk size larger than the body actually received. This results in a heap-buffer-over-read. This issue has been patched in version 1.0.5.	N/A	More Details
CVE-2026-65843	sync-rpc runs asynchronous commands synchronously by putting them in a separate proces. Prior to version 1.3.7, if an attacker could guess the correct port and it was not blocked via a firewall, it was possible to load and execute arbitrary JavaScript files stored on the server running sync-rpc. This issue has been patched in version 1.3.7.	N/A	More Details
CVE-2026-116835	In affected versions of Octopus Server, insufficient validation of custom claims on OIDC accounts allowed a user with permission to edit accounts to cause Octopus Server to issue signed OIDC tokens that impersonate a different project. This could grant access to external systems, such as cloud providers or other Octopus instances, that trust that project's identity.	N/A	More Details
CVE-2026-128131	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, aiohttp decompresses each member of a payload containing many concatenated gzip, deflate, or zstd streams by passing the entire remaining input to a new decompressor, causing quadratic CPU use. Empty members produce no output, so client_max_size and output backpressure do not limit the work. A remote attacker can block a server event loop with a crafted compressed request body or WebSocket message, and a malicious server can similarly block a client. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-124627	In affected versions of Octopus Server, incorrect validation of the external identity linked to a newly registered user could result in that user receiving the LDAP-mapped team memberships and associated permissions of another user. This issue only affects instances with LDAP authentication enabled and LDAP groups mapped to Octopus teams.	N/A	More Details
CVE-2026-59075	Edito CMS is vulnerable to Dynamic LINQ injection. Due to improper input validation, an authenticated attacker can inject conditional expressions into the sort parameter of paginated administrative endpoints. Analyzing the returned result order allows the attacker to extract value of any field character by character, leading to potential exposure of sensitive data. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-111338	Sensitive authentication material written to a log file in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111339	Memory overflow in Application Firewall data decompression/inspection can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details

CVE-2026-120860	Memory overflow in protocol load-balancing traffic handling (Diameter, SIP-over-TCP, MQTT, RADIUS) can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-120861	Memory overflow / improper handling in GSLB and geolocation (MEP, static-proximity, config-sync) can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-120862	Memory overflow in SIP ALG (LSN) and DNS answer-section logging datapaths can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-120863	Memory overflow in the management plane can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-128637	The MISP Modules website component contains an open redirect vulnerability in its login endpoint. The /login route accepted a user-supplied next query parameter and passed it directly to Flask's redirect() function without validating the destination. An attacker could craft a URL such as https://victim-host/login?next=https://attacker.example/phish and deliver it to a user (e.g., via email or a lookalike page). After the user successfully authenticated, the application issued a 302 redirect to the attacker-controlled external URL. This enables phishing attacks where a user, believing they are still on the legitimate MISP Modules site, may enter additional credentials or sensitive information on the attacker's page. It can also be used to obscure the true destination of a link, bypassing user trust in the legitimate domain. The vulnerability requires the victim to interact with the crafted URL and complete a login, but no prior authentication or special configuration is needed on the attacker's side. The affected component is the website sub-project of misp-modules, specifically the account blueprint in website/app/account/account.py. No version boundaries are specified in the patch metadata.	N/A	More Details
CVE-2026-59074	Edito CMS is vulnerable to improper cryptographic signature verification in the JWT refresh logic. An authenticated low-privilege user can submit self-crafted JWT containing an existing user identifier and, due to the lack of signature validation, obtain a valid, fully-signed session token for any account in the system. This allows the attacker to impersonate any user, including administrators. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-59076	Edito CMS is vulnerable to Stored Cross-Site Scripting (XSS). Due to improper input validation, an authenticated attacker can inject malicious scripts into givenName and surname parameters via the /api/auth/profile endpoint. When an administrator visits the admin changelog logs, the injected script is automatically executed, in his browser. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-103645	An integer overflow vulnerability in the Qt QTextCodec fromUnicode() and toUnicode() functionality of the Qt 5 Core Compatibility APIs module (Qt 6) and the Qt Core module (Qt 5). Only builds where Qt is compiled with ICU support are affected.	N/A	More Details
CVE-2026-59077	Edito CMS is vulnerable to Stored XSS via content parameter in Tiny editor functionality. Authenticated attacker can inject arbitrary HTML and JS into website, which will be rendered/executed when user tries to edit changed entry. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-59078	Edito CMS is vulnerable to Stored XSS in avatar upload functionality. Authenticated attacker can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting an URL leading to a edited avatar. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-59079	Edito CMS restricts the ability to upload files via the UI to specific file types. However, an avatar upload functionality allows an attacker to upload files of any type and extension without restriction. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-59080	Edito CMS sends JWT token via GET requests. This allows a local attacker with access to browser history to obtain valid JWT token and perform action on behalf of the victim. The token is valid for only short period of time; after that time, it expires and can no longer be used. The vendor assessed the likelihood of exploitation as very low and determined that a fix is not necessary.	N/A	More Details
CVE-2026-59081	Edito CMS deserializes JSON data without further validation. A user (even an administrator) cannot exploit this vulnerability through the application's normal functionality. An attacker who could modify cache entries or inject them could execute code on the server. This issue was fixed in version 5.10.2607. Hotfixes for older versions (5.8) have also been released.	N/A	More Details
CVE-2026-120864	Memory overflow in ICA proxy can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-120865	Memory overflow in HTTP/3 (QUIC) can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details

CVE-2026-120866	Memory overflow / improper handling in BGP dynamic routing can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111337	Memory overflow in Base64 decoding in advanced policy expressions leading to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111336	Memory overflow in HTTP/2 handling can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111335	Improper request handling can lead to a denial-of-service / reboot-loop condition in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111334	Memory overflow in Endpoint Analysis (EPA/EPAS) can lead to unpredictable or erroneous behavior or a Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-107411	Memory overflow in RTSP ALG can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-107412	Multiple Memory overflow vulnerabilities can lead to unpredictable or erroneous behavior and Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-107413	Memory overflow in SAML authentication can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-107414	Memory overflow in WebAuth authentication can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-107415	Memory overflow in Email OTP authentication can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-124726	Relative Path Traversal, with Unintended Proxy vulnerability in Apache APISIX. A caller of the MCP endpoint can invoke endpoints the OpenAPI document never declared, under the declared tool's HTTP method, using the credentials the Route adds. This issue affects Apache APISIX: from 3.19.0 before 3.20.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-2026-124723	Interpretation Conflict, leading to Incorrect Authorization vulnerability in Apache APISIX. With match_uri_encoded_slash enabled and skip_mtls_uri_regex configured, a client without a certificate can reach an upstream behind a route that requires one, limited to request paths that decode to an exempted URI. This issue affects Apache APISIX: from 3.18.0 through 3.19.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-2026-124719	Authentication bypass by spoofing vulnerability in Apache APISIX. When a Route's configured headers carry a caller identity and the OpenAPI document declares the same header, a caller can act as another identity against the upstream API. This issue affects Apache APISIX: from 3.19.0 before 3.20.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-2026-124716	Incorrect Authorization vulnerability in Apache APISIX. An authenticated user who holds any one of a route's required permissions or scopes can reach the protected upstream without the others, including HTTP methods the authorization server denied. This issue affects Apache APISIX: from 1.4.0 through 3.19.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-2026-124680	Interpretation Conflict, resulting in (Incorrect Authorization) vulnerability in Apache APISIX. An unauthenticated client can reach upstream paths protected by a route-level auth plugin when a route without auth exists on the same upstream and the upstream does not collapse encoded dot segments. This issue affects Apache APISIX: from 0.9 through 3.19.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-2026-124679	Authentication bypass by spoofing vulnerability in Apache APISIX. On routes using jwe-decrypt with strict: false and a forward_header distinct from the token header an unauthenticated client can supply the value the upstream treats as gateway-decrypted plaintext. Similar can happen when forward-auth is configured with allow_degradation: true, and the auth service is unavailable. This issue affects Apache APISIX: from 3.18.0 through 3.19.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	More Details
CVE-	Authentication bypass by spoofing vulnerability in Apache APISIX. On a route where multi-auth falls back from wolf-rbac to another successful authenticator, client-supplied Wolf identity headers can remain in the request. A		More

2026-124666	downstream service that relies on those documented headers may therefore receive an identity that was not established by the successful authenticator. This issue affects Apache APISIX: from 3.8.0 through 3.19.0. Users are recommended to upgrade to version 3.20.0, which fixes the issue.	N/A	Details
CVE-2026-111340	Memory overflow in KBA (knowledge-based authentication) can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111341	Memory overflow in client-certificate authentication can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-107398	Indico is a feature-rich event management system. Prior to version 3.3.14, due to a path traversal vulnerability when building an "offline copy" of an event, a malicious event manager has the ability to retrieve the content of any local file that's readable by the user running Indico on the server. This issue has been patched in version 3.3.14.	N/A	More Details
CVE-2026-111342	Memory overflow in LDAP authentication can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-111333	Memory overflow in an authentication request can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-120867	Memory overflow in SSL/TLS/DTLS can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler ADC and Citrix NetScaler Gateway.	N/A	More Details
CVE-2026-128986	In Eclipse BaSyx Go Components versions up to and including 1.1.3, ABAC-enabled deployments match `ROUTE` access rules against the fully decoded request path, while the router routes on the raw, still encoded path. An encoded slash (`%2F`) inside a path value is a segment separator for the access check but part of the value for the router, so a request can match a narrow `ROUTE` rule while the handler returns a different, larger resource. An authenticated caller whose rules grant READ only on parts of a resource can therefore read the whole resource. In the DPP API, a rule such as `/v1/dpps/*/elements/*`, meant to grant only passport elements, also grants the complete passport whose identifier contains `/elements/`. In the Submodel Repository, AAS Repository and AAS Environment, a rule such as `/submodels/*/submodel-elements/*/attachment`, meant to grant only file attachments, also grants the complete element whose stored idShort contains `%2F`. The issue is fixed in Eclipse BaSyx Go Components v1.1.4.	N/A	More Details
CVE-2026-124628	In affected versions of Octopus Server, incorrect validation of changes a user made to their own LDAP identity allowed them to edit that identity even when an Administrator had disabled self-service identity editing. This could result in the user gaining membership of teams mapped to external LDAP groups they do not belong to, and potentially escalating to full administrative privileges if any of those teams are privileged.	N/A	More Details
CVE-2026-124760	P-Net before 1.0.4 sets the alarm receiver state to waiting for confirmation before the data of a received alarm notification is parsed. If the parsing fails the state is not restored, and later alarm notifications of the same priority are discarded without acknowledge until the Application Relationship is released. The Application Relationship and the cyclic data exchange keep working. The attacker must be able to send an alarm notification in the context of an established Application Relationship and requires ADJACENT network access.	N/A	More Details
CVE-2026-105622	Improper restriction of excessive authentication attempts in the WAMP-CRA (challenge-response) authentication path in Zenitel Connect before 1.11.0 allows remote attackers to guess user passwords via unlimited authentication attempts, because the path, in which the broker issues a challenge and the client returns an HMAC of it keyed with the user's secret, applies no account lockout or rate limiting. Affected releases enforce a password policy of at least 12 characters including upper-case, lower-case, numeric and special characters, so practical exploitation requires a reused or predictable password rather than exhaustive guessing. The WAMP-CRA authentication path is removed in 1.11.0.	N/A	More Details
CVE-2026-109904	A buffer overread caused by an integer-overflow in Proc/SProcXResQueryClientIds in X.Org xwayland before 24.1.15 and X Server before 21.1.26 could be used by attackers on authenticated X clients to crash the server or leak out information.	N/A	More Details
CVE-2026-112182	Unauthorization vulnerability in the management of workflow definitions in OpenKM Community Edition. The REST endpoints `registerProcessDefinition` and `runProcessDefinition` require authentication but do not verify roles in the WorkflowService or in lower layers. An attacker with the `ROLE_USER` role can register and execute a process definition containing BeanShell scripts, allowing them to execute Java code and operating system commands with the service’s privileges. In the official Docker image, the process runs as root.	N/A	More Details
CVE-2026-125659	This vulnerability exists in the eMudhra emBridge due to missing authorization checks in the FileBrowser API endpoints. These endpoints perform file system enumeration using the LocalSystem account without adequately validating the requesting caller's authorization. An unauthenticated attacker on the same LAN could exploit this vulnerability by sending malicious webpage to the local HTTPS Web API. Successful exploitation of this vulnerability could allow the attacker to enumerate file and directory names and obtain information about the	N/A	More Details

	directory structure of the targeted system. The vulnerability however, does not provide access to file contents or permit file modification, deletion, or code execution, or access to cryptographic keys and hardware token PINs.		
CVE-2026-120221	In FRRouting, bgpd frees the same memory twice when dynamic BGP neighbors disconnect, if the peer-group used by a "bgp listen range" also has a Site-of-Origin configured ("neighbor PG soo"). Each dynamic neighbor shares the peer-group's SoO value instead of getting its own copy, but frees it as its own when the neighbor is deleted, which happens as soon as its connection closes. The first disconnect leaves the peer-group pointing at freed memory, and the second disconnect frees it again, causing bgpd to abort and drop all BGP sessions on the router. Any host whose address falls inside the listen range can trigger this by opening and closing two TCP connections to the BGP port, without sending any BGP message and without knowing the AS number, and can repeat it each time bgpd restarts. If the peer-group has a TCP-MD5 password, only hosts that know the password can trigger it. Two ordinary flaps of legitimate dynamic neighbors have the same effect. Between the two frees, displaying the configuration ("show running-config") or establishing a dynamic neighbor also reads the freed memory, which can crash bgpd after a single disconnect. Only configurations that combine a listen range with a SoO on the same peer-group are affected.	N/A	More Details
CVE-2026-109095	A integer overflow in glamor Xv Image Size handling in X.Org xwayland before 24.1.15 and X server before 21.1.26 could be used by authenticated clients to crash the X server or leak out data.	N/A	More Details
CVE-2026-124758	P-Net before 1.0.4 does not check the record data length of an IODWrite request to a non-user record index against the size of the record block header. The 32-bit length is reduced by the header size before it is passed to the record handlers, so a length smaller than the header underflows and the handlers receive a data length of about 65530. The fixed-size reads of the I&M and PDPort handlers can then read past the end of the session buffer. The result of the write is discarded. The attacker must have an established Application Relationship or be able to send in the context of one, and requires ADJACENT network access.	N/A	More Details
CVE-2026-124759	P-Net before 1.0.4 routes a received RTA alarm frame to an Application Relationship using only the destination alarm reference in the frame, without checking the source of the frame. A host with ADJACENT network access can abort an established Application Relationship with a single alarm ERROR frame, or deliver forged alarm notifications with chosen type, slot, subslot, USI and payload to the application.	N/A	More Details
CVE-2026-127102	In Eclipse BaSyx Go Components versions up to and including 1.1.2, ABAC-enabled deployments of the Submodel Repository and the AAS Environment return Submodel Elements that the caller is not authorized to read from `GET /submodels/{submodelIdentifier}/submodel-elements`. If an access rule grants READ on a single Submodel Element through a `$sme` `REFERABLE` object, the list route returns every element of that Submodel, including its value, as soon as one element matches the caller's rules. The single-element route and the full Submodel read enforce the same rule and deny access to the other elements. An authenticated caller with a READ grant for one element of a Submodel can therefore read all other elements of that Submodel. The issue is fixed in Eclipse BaSyx Go Components v1.1.3.	N/A	More Details
CVE-2026-124279	Allocation of Resources Without Limits or Throttling vulnerability in elixir-grpc grpc_server allows unauthenticated attackers to exhaust server memory via client-streaming or bidirectional-streaming requests. The streaming read clause of GRPC.Server.Adapters.Cowboy.Handler.info/3 (grpc_server/lib/grpc/server/adapters/cowboy/handler.ex) asks Cowboy for up to 8,000,000 bytes per read and compares the running total with max_body_size only after the read returns. The gRPC length prefix of a message is not checked before the message is buffered. Each stream can therefore buffer up to one full read beyond the configured limit before it is refused, and many concurrent streams exhaust node memory. Releases before 1.0.6 apply no limit to streaming requests at all. This issue affects grpc_server: from 1.0.0 before 1.1.0.	N/A	More Details
CVE-2026-127031	In Eclipse AAS4J before 3.0.1, `XmlSchemaValidator.validateSchema()` (and `AASXValidator.validateSchema()`, which calls it) validates untrusted XML with a default JAXP `Validator` that resolves external DTDs and external entities. An attacker who supplies a crafted AAS XML document or AASX package can read local files from the host, send their contents out-of-band to an attacker-controlled server, and make the validating process send arbitrary outbound requests (SSRF). Validation still returns no errors. Details: - Vulnerable code: `dataformat-xml/src/main/java/org/eclipse/digitaltwin/aas4j/v3/dataformat/xml/XmlSchemaValidator.java`. `schema.newValidator().validate(new StreamSource(...))` runs without `ACCESS_EXTERNAL_DTD` / `ACCESS_EXTERNAL_SCHEMA` restrictions and without `disallow-doctype-decl`. - Second entry point: `dataformat-aasx/src/main/java/org/eclipse/digitaltwin/aas4j/v3/dataformat/aasx/AASXValidator.java`. The AAS XML part of an `.aasx` package is passed unchanged to the vulnerable validator. - `XmlDeserializer` (Jackson/Woodstox) is not affected, because DTD support is disabled by default there. - Present since the initial import of the code base (commit `cc9da52`). - Fix: harden the validator by setting `ACCESS_EXTERNAL_DTD` and `ACCESS_EXTERNAL_SCHEMA` to `""` and rejecting `DOCTYPE` declarations. The bundled `AAS.xsd` does not need DTDs, so no functionality is lost.	N/A	More Details
CVE-2026-124761	P-Net before 1.0.4 copies the IP suite of a DCP Set request to the current and the non-volatile configuration, and starts saving it, before the state of the device is checked. If the request is refused, for example because an Application Relationship is active, the configuration is not restored and is still saved. After a restart the device uses the refused address, and may not answer the controller or may use its address. A host with ADJACENT network access can use this while an Application Relationship is active.	N/A	More Details
CVE-	P-Net before 1.0.4 finds the RPC session of a received PDU by its activity UUID only, and a reject, fault or cancel PDU for the session aborts the Application Relationship, without checking that the PDU is the answer to a call of		

2026-124762	the device or where it comes from. A host with ADJACENT network access that has observed the activity UUID of the connection, which is sent in clear in every RPC request, can abort the Application Relationship with one PDU. It also allocates a session for an unknown activity UUID and changes the address stored for an existing session.	N/A	More Details
CVE-2026-127122	P-Net before 1.0.4 does not check the number of MCR request blocks in a Connect request against the number of multicast communication relations that an Application Relationship has room for (PNET_MAX_MC_CR, 1 by default). Each further block is written past the end of the array, into the rest of the Application Relationship and, with more blocks, into the following one. The written data comes from the request. No established Application Relationship is needed, and the attacker requires ADJACENT network access. Builds with PNET_OPTION_MC_CR disabled are not affected.	N/A	More Details
CVE-2026-127123	P-Net before 1.0.4 releases the Application Relationship of an RPC session, without the abort procedure, when a fragment of a request has another data representation (endianness) than the first fragment of the call. The application is not told that the Application Relationship is gone, the cyclic data stops, and the resources of the Application Relationship are left referencing a cleared structure. Another host can then connect in its place. A host with ADJACENT network access that has observed the activity UUID of the connection, which is sent in clear in every RPC request, can do this with one PDU.	N/A	More Details
CVE-2026-127124	P-Net before 1.0.4 keeps the RPC session that is allocated for a fragment of a request with an unknown activity UUID, without a timeout, when the rest of the request never arrives. A session that does not get an Application Relationship is also kept after the response. Repeated fragments or requests with different activity UUIDs exhaust the available sessions, one UDP packet per session. Once they are exhausted the device no longer answers a Connect request until it is restarted. An unauthenticated attacker with ADJACENT network access can use this to cause a denial of service.	N/A	More Details
CVE-2026-127125	P-Net before 1.0.4 aborts the Application Relationship of an RPC session when a fragment of a response has been resent without being acknowledged, without checking that the session has an Application Relationship. A request for an existing Application Relationship that is sent on another activity than its Connect, and gets a fragmented response, is handled on a session without one. If the response is not acknowledged, a NULL pointer is dereferenced and the device crashes. A conformant IO-controller does not send such requests. The attacker must have observed the AR UUID of an established Application Relationship and requires ADJACENT network access.	N/A	More Details
CVE-2026-128790	In Eclipse BaSyx Go Components versions up to and including 1.1.2, ABAC-enabled deployments of the Submodel Repository and the AAS Environment do not apply an access rule's `FILTERLIST` fragment filters to single Submodel reads. `GET /submodels` removes the fields that a rule's `FILTERLIST` hides, but `GET /submodels/{submodelIdentifier}` and `GET /submodels/{submodelIdentifier}/$metadata` return them unfiltered. An authenticated caller with READ access to a Submodel can therefore read fields that the access rules hide from them, for example `supplementalSemanticIds` keys that name the other parties allowed to read the Submodel. If versioning is enabled (`history.mode` set to `api` or `audit`), `GET /submodels/{submodelIdentifier}/$history` and `GET /shells/{aasIdentifier}/$history` in the Submodel Repository, AAS Repository and AAS Environment return the complete stored version without applying the rule's formula or fragment filters. A caller whose rules grant READ on these routes can read fields that the access rules hide, and Submodels and Asset Administration Shells that the direct read does not return to them at all. The issue is fixed in Eclipse BaSyx Go Components v1.1.3.	N/A	More Details
CVE-2026-105623	The web interface in Zenitel Connect before 1.11.0 serves production JavaScript source maps without authentication, which allows remote attackers to obtain the complete front-end source code, including API usage and internal client logic, via requests for the source map files.	N/A	More Details
CVE-2026-105624	The login flow in Zenitel Connect before 1.11.0 applies per-account lockout on repeated failed login attempts, which allows remote attackers to cause a denial of service (temporary lockout of targeted user accounts from the web interface, repeatable for as long as the attack continues) via repeated failed login requests for a known or guessed username. Intercom call handling is not affected.	N/A	More Details
CVE-2026-105625	The web interface in Zenitel Connect before 1.11.0 loads an integration iframe without sandboxing or origin restrictions, which allows remote attackers to present phishing content to authenticated users via a crafted frame source.	N/A	More Details
CVE-2026-105671	The login flow in Zenitel Connect before 1.11.0 returns different error responses depending on whether a submitted username exists, which allows remote attackers to enumerate valid user accounts via crafted login requests.	N/A	More Details
CVE-2026-121809	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in elixir-grpc grpc_server and grpc allows unauthenticated attackers to occupy a BEAM scheduler indefinitely via a client-streaming or bidirectional-streaming request whose body ends inside a gRPC message. GRPC.Server.Adapters.Cowboy.read_stream/1 (grpc_server/lib/grpc/server/adapters/cowboy.ex, and the Cowboy adapter in grpc before the package split) asks for more data whenever the buffer does not hold a complete message. Once the request body has ended, every further read returns an empty chunk, so the buffer never changes and the function retries without end. A single 5-byte length prefix sent with END_STREAM keeps one scheduler busy for as long as the connection stays open, and repeated requests exhaust all schedulers. This issue affects grpc_server: from 1.0.0 before 1.1.0; grpc: from 0.3.1 before 1.0.0.	N/A	More Details

CVE-2026-95615	OS command injection vulnerability in audio messages API in Zenitel Connect before 1.11.0 allows remote authenticated users to execute arbitrary OS commands as root in the hiatus application container via filename parameter to the /api/system/audio_messages endpoint.	N/A	More Details
CVE-2026-95614	The host configuration watcher in Zenitel Connect before 1.11.0 applies a rsyslog configuration file written to a data volume that is shared with the hiatus application container, which allows local attackers with write access to the hiatus container filesystem to execute arbitrary OS commands as root on the host operating system via a crafted rsyslog configuration file.	N/A	More Details
CVE-2026-95613	The pREST database REST API in Zenitel Connect firmware before 1.11.0 signs and verifies JWTs with the platform CA private key, which is stored on a data volume shared between containers, and sets the PostgreSQL session role from the unvalidated sub claim of each request while connected to the database as the "postgres" superuser, which allows local attackers who can read the platform CA private key from the container filesystem to execute database operations as the PostgreSQL superuser, including reading the master encryption key and password hashes, via a forged JWT with sub=postgres sent to the pREST API.	N/A	More Details
CVE-2026-95379	Path traversal in the certificate.deleteCertificate JSON-RPC method (POST /api/rpc) of the turbineweb web interface in Zenitel VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices with software versions from 10.0.3.0 before 10.1.3.0 allows authenticated administrators to delete arbitrary files as root via a relative path (../) in the file_name parameter. This can be used to cause denial of service or render the device inoperable by removing critical system files, and to weaken device security by removing files such as firewall rules or certificate trust stores.	N/A	More Details
CVE-2026-95378	Path traversal in the certificate upload endpoint (/api/certificate/upload) of the turbineweb web interface in Zenitel VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices with software versions from 10.0.3.0 before 10.1.3.0 allows authenticated administrators to write arbitrary files as root via a crafted filename parameter in a multipart upload request when the type field is set to any value other than https_certificate. In that case, both path validation and certificate content validation are skipped. This can be escalated to arbitrary code execution as root, for example by overwriting startup scripts or planting SSH keys.	N/A	More Details
CVE-2026-95377	OS command injection in the TFTP provisioning module of Zenitel EdgeAudioClient before 9.6.3.0, and 10.x before 10.1.3.0, on VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices allows unauthenticated adjacent attackers to execute arbitrary commands as root via a crafted DHCP option 66 (TFTP Server Name) value supplied by a rogue DHCP server on the same network segment. The DHCP-supplied value is passed to a shell without sanitization. Devices using DHCP, the default configuration, are affected on every boot and lease renewal. The same injection is also reachable via the config_update_tftp_server and sw_update_tftp_server configuration fields by an attacker able to modify the device configuration.	N/A	More Details
CVE-2026-112181	Vulnerability due to inadequate restriction of references to external XML entities in OpenKM Community Edition. The XML processing in FormUtils / LocalEntityResolver does not properly restrict the resolution of external resources. An authenticated remote attacker with the ROLE_USER role can exploit the flaw via a REST request. In the 6.3.x branch, this allows the attacker to trigger HTTP requests under their control (SSRF); in 7.0.3, it allows the attacker to read local files and access internal HTTP resources from the server.	N/A	More Details
CVE-2026-62974	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, a malformed but non-empty BACnet WriteProperty request can drive the official server demo into a non-terminating request-processing loop with repeated heap-backed side effects. This results in a remote unauthenticated denial of service via uncontrolled resource consumption and a non-terminating request path. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	N/A	More Details
CVE-2026-62972	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, lighting_command_decode in src/bacnet/lighting.c decodes its first field with the bounded apdu_size - apdu_len, but every nested decode in the operation switch is called with the original full apdu_size while the read pointer has been advanced to &apdu[apdu_len]. The leaf decoders bound their reads against the size they are told, so they read up to apdu_len bytes past the end of the caller's buffer, resulting in an out-of-bounds read. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	N/A	More Details
CVE-2026-52788	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.5, 1.5.1, and 1.6.0, the bsc_node_parse_urls() function in src/bacnet/datalink/bsc/bsc-node.c contains three distinct bugs when parsing space-separated WebSocket URIs from a BACnet/SC Address Resolution ACK message. Two bugs cause out-of-bounds writes past the utf8_urls[10][129] array in the static BSC_ADDRESS_RESOLUTION structure. This issue has been patched in versions 1.4.5, 1.5.1, and 1.6.0.	N/A	More Details
CVE-2026-126949	Zipline through 4.4.0 contains a path traversal vulnerability in the PATCH /api/user/files/:id rename endpoint that allows authenticated users to overwrite existing uploads by supplying unsanitized names. Attackers can submit names like ../uploads/victim.txt that bypass the raw-string database uniqueness check but normalize via path.join(), causing fs.rename() to replace other files' contents.	N/A	More Details
CVE-2026-126950	Zipline through 4.4.0 contains a path traversal vulnerability that allows authenticated attackers to delete arbitrary server files by injecting traversal sequences via the x-zipline-file-extension header. Attackers can upload a file with a poisoned stored name and short expiry so LocalDatasource deletion removes chosen files, causing denial of service or data loss.	N/A	More Details

CVE-2026-126951	Zipline through 4.4.0 contains a path traversal vulnerability that allows authenticated users to read arbitrary server files by abusing a fallback treating the :id parameter as a datasource key. Attackers can send encoded traversal sequences in the :id of GET /api/user/files/:id/raw to escape the Local datasource uploads directory and read files like /etc/shadow.	N/A	More Details
CVE-2026-124278	Authorization Bypass Through User-Controlled Key vulnerability in elixir-grpc grpc_server and grpc allows an attacker to make a handler act on a resource other than the one named in the URL of an HTTP-transcoded route, via a request with a gRPC Content-Type. Only the transcoding clause of GRPC.Server.do_handle_request/4 (grpc_server/lib/grpc/server.ex, and lib/grpc/server.ex before the package split) applies the route's path bindings to the request message. The Cowboy handler picks that clause from the request Content-Type, not from the route. A request to a transcoded URL with application/grpc or application/grpc-web is decoded from the body alone, so every path-bound field takes its value from the body. A gateway, proxy rule or WAF that authorizes on the URL path sees one resource while the handler receives another. This issue affects grpc_server: from 1.0.0 before 1.1.0; grpc: from 0.8.0 before 1.0.0.	N/A	More Details
CVE-2026-123635	Missing Release of Resource after Effective Lifetime vulnerability in elixir-grpc grpc_server allows a client to stall all later calls on a shared HTTP/2 connection via calls that the server refuses while their DATA frames are in flight. The stream handler grpc_stream_h (grpc_server/src/grpc_stream_h.erl) requests flow from Cowboy only for request data that has arrived. When the server refuses a call early, for example because the body exceeds max_body_size or the method is not implemented, Cowboy drops the DATA frames still in flight for that stream. Their bytes are not returned to the connection flow-control window. After enough refused calls the window is empty. No call on that connection can then send a request body, and each call waits until its deadline. Other connections are not affected. This issue affects grpc_server: from 1.0.0 before 1.1.0.	N/A	More Details
CVE-2026-121808	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in elixir-grpc grpc_core and grpc allows unauthenticated attackers to exhaust server memory via a compressed Erlang external term in a gRPC message body. GRPC.Codec.Erlpack.decode/2 (grpc_core/lib/grpc/codec/erlpack.ex, and lib/grpc/codec/erlpack.ex before the package split) passes the message body to :erlang.binary_to_term/2. That function inflates a compressed term in full before it returns. The codec sets no limit on the decoded size, and its type checks run only on the decoded term. The server's max_body_size limit counts the compressed bytes of the request. A request with Content-Type: application/grpc+erlpack can therefore make the server allocate a term much larger than the request body. This issue affects grpc: from 0.4.0 before 1.0.0; grpc_core: from 1.0.0 before 1.1.0.	N/A	More Details
CVE-2026-128074	Nuxt is an open-source web development framework for Vue.js. From 4.6.0 until 4.6.4, _payload.json URL generation and the experimental early-404 path use a trailing-slash regular expression whose work grows quadratically with a long run of slash characters. An unauthenticated request can synchronously occupy the Node.js event loop and delay other requests when server-side rendering uses isr, swr, or cache route rules, or when experimental.early404 is enabled. Applications without those route rules and without experimental.early404, fully prerendered applications, and client-only applications are unaffected; the impact is limited to availability. This issue is fixed in version 4.6.4.	N/A	More Details
CVE-2026-128078	GLPI is a free asset and IT management software package. From 9.5.0 until 10.0.27 and 11.0.9, authenticated users could access ITIL followups, tasks, or solutions generated from templates without a read-permission check on the parent ticket, problem, or change. Depending on the template configuration, this could reveal information from parent items the user could not otherwise read. This issue is fixed in versions 10.0.27 and 11.0.9.	N/A	More Details
CVE-2026-128079	envd provides reproducible development environments for humans and agents. In versions starting with 0.3.38 and before 1.3.6, insufficient containment of host-side requirements-file reads in install.python_packages(requirements=...) could allow access to files outside the build context. An attacker able to influence build input could cause file contents interpreted as dependency entries to appear in debug logs or build-step metadata, subject to the envd process's permissions. Exploitation in version 1.3.5 additionally requires concurrent modification of relevant filesystem paths. This issue is fixed in version 1.3.6.	N/A	More Details
CVE-2026-118495	Joomla / WordPress Extension - acymailing.com - Exposure of sensitive information to an unauthorized actor in AcyMailing 6.0.0 - 11.1.1 - Exposure of sensitive information to an unauthorized actor in AcyMailing 6.0.0 through 11.1.1. An unauthenticated attacker who knows a subscriber's email address can read that subscriber's record, including the per-subscriber secret key that authorises the subscription management links. Holding that key, the attacker can act as that subscriber on those endpoints, which includes triggering the GDPR data export and the GDPR account deletion where those options are enabled.	N/A	More Details
CVE-2026-128126	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, Request.post() does not limit the number of fields in a URL-encoded form body, and inserting many repeated keys into MultiDict takes quadratic time on the event loop. A remote attacker can send a form POST within client_max_size to a handler that calls Request.post() and block the event loop. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-128125	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, Set-Cookie parsing treats unrecognized name=value attributes as additional cookies, while CookieJar does not limit the number of cookies stored or sent. A malicious server can make an aiohttp client accumulate a very large cookie set, consume memory and CPU repeatedly across redirects, and construct an excessively large Cookie header for later requests to the same domain. This issue is fixed in version 3.14.4.	N/A	More Details

CVE-2026-128124	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, Application.add_domain() converts every asterisk wildcard in a domain mask into a greedy regular-expression fragment, so a mask containing two or more wildcards can take polynomial time to reject a long Host header that does not match. A remote attacker can repeatedly send such headers to a server configured with a multi-wildcard domain mask and stall the event loop. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-117543	Joomla Extension - jdownloads.com - SSRF via external download URL field jDownloads < 4.1.8 - HTTP redirects when retrieving external download URLs could bypass validation of the original destination. This allowed server-side requests to internal or otherwise prohibited destinations and disclosure of their responses (SSRF).	N/A	More Details
CVE-2026-117550	Joomla Extension - jdownloads.com - Publishing of files without approval in jDownloads < 4.1.8 - Manipulated frontend submission parameters could bypass the intended publication and ownership rules. In particular, submissions could be published despite automatic publication being disabled, and ownership could be assigned contrary to the intended policy.	N/A	More Details
CVE-2025-43867	- Dependency on Vulnerable Third-Party Component vulnerability in Johnson Controls FX Server, Johnson Controls FX80, and Johnson Controls FX90 allows CAPEC-17: Accessing, Modifying or Deleting Files. This issue affects FX Server: before 14.10.10 and before 14.14.1; FX80: before 14.14.10 and before 14.14.1; FX90: before 14.10.10 and before 14.14.1.	N/A	More Details
CVE-2026-117551	Joomla Extension - jdownloads.com - RCE through file upload in jDownloads < 4.1.8 - Insufficient validation of frontend thumbnail uploads allowed users with upload permission to place executable files on the server. This results in PHP code execution.	N/A	More Details
CVE-2026-68551	Budget Board is an app for tracking monthly spending and working towards financial goals. Prior to version 3.6.2, Budget Board's OIDC login flow finds and signs into an existing local account purely by matching the email address asserted in the identity provider's token - it never checks the standard email_verified claim. If the configured OIDC provider ever allows a user to register or display an email address without proving they own it , an attacker can register there using a victim's email and get signed into the victim's existing Budget Board account - including all their linked bank data. This issue has been patched in version 3.6.2.	N/A	More Details
CVE-2026-119275	Akaunting 3.3.0 contains a stored cross-site scripting vulnerability in the XLSX invoice-import workflow. An authenticated Manager can import a child invoice whose invoice number contains HTML and is linked to a recurring invoice. When a victim opens that recurring invoice, Akaunting raw-renders the stored child number in an anchor, causing attacker-controlled markup to execute in the victim's browser.	N/A	More Details
CVE-2026-107410	Memory overflow in NetScaler Push can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-120466	Joomla / WordPress Extension - acymailing.com - Missing authorization on subscription changes in AcyMailing 1.0.0 - 11.1.1 - An unauthenticated attacker who knows a subscriber's email address can unsubscribe that subscriber from one mailing list or from every mailing lists, without proving that the address is theirs. The affected feature also lets an attacker determine whether a given email address belongs to a subscriber of the site.	N/A	More Details
CVE-2026-120468	Joomla Extension - acymailing.com - Unauthenticated disclosure of mailing list metadata in AcyMailing 1.0.0 - 11.1.1 - An unauthenticated attacker can retrieve every mailing list of the site, including lists that are not publicly visible and lists restricted to an access level, together with their descriptions, access levels, owning user account and subscriber counts. The WordPress plugin is not affected.	N/A	More Details
CVE-2026-120469	Joomla / WordPress Extension - acymailing.com - Open redirect on the subscription and unsubscription endpoints in AcyMailing 1.0.0 - 11.1.1 - On a default configuration, an attacker can craft a link on the affected site that redirects the visitor to an arbitrary external site, which is usable for phishing under the trusted domain.	N/A	More Details
CVE-2026-120470	Joomla / WordPress Extension - acymailing.com - Online version of an email readable without the visibility check in AcyMailing 1.0.0 - 11.1.1 - An unauthenticated attacker can read the online version of campaigns that were never made public, including campaigns unpublished after being sent and campaigns sent to a restricted audience.	N/A	More Details
CVE-2026-120471	Joomla Extension - acymailing.com - Site modules rendered outside their access level in AcyMailing 1.0.0 - 11.1.1 - An unauthenticated visitor can cause a site module to be rendered regardless of the Joomla access level that module is restricted to, which discloses content reserved for a higher view level. The WordPress plugin is not affected.	N/A	More Details
CVE-2026-125324	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-127063	The third-party RMM+ extension for ConnectWise ScreenConnect uses a static API secret by default. The value can be changed by an administrator; however, environments retaining the default value may allow unauthorized access to extension API functionality, including the ability to send commands to managed agents. This issue is specific to the third-party extension and does not affect the ScreenConnect server or client. Scope: This issue affects the third-party RMM+ extension for ConnectWise ScreenConnect. Deployments without the extension are not affected. ScreenConnect server or client software are not impacted.	N/A	More Details

CVE-2024-21954	Improper exception handling in IOMMU could allow an invalidate command to be sent to PCIe devices that do not support Address Translation Cache (ATC), potentially resulting in denial of service.	N/A	More Details
CVE-2026-128127	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, BodyPartReader.read_chunk() processing a multipart part with Content-Transfer-Encoding set to base64 keeps reading until the chunk length is a multiple of four without enforcing a byte limit. A short Content-Length or a long run of whitespace can cause one call to read the remaining body into memory before the size check or spin on the event loop. A remote attacker can send such a multipart request to a handler that reads multipart data and bypass client_max_size. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-107365	A user with query access to a Google Cloud Monitoring data source can use its resource proxy to send requests to other Cloud Monitoring API paths with the data source's credentials, and read data from any project those credentials can reach. When the data source forwards the user's OAuth identity or uses Workload Identity Federation, the impact depends on that credential's permissions. Fixed in Google Cloud Monitoring plugin 12.6.7.	N/A	More Details
CVE-2026-128129	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, aiohttp buffers all additional connection data received while a request marked for upgrade, such as a WebSocket handshake, is being handled, without a size limit or flow control. A remote attacker can stream data behind an upgrade request to a handler that does not immediately accept or reject the upgrade and cause unbounded memory consumption. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-128130	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, when the pipelined request queue is full, the pure-Python parser stores the unparsed remainder internally and also returns the same data to its caller. After a handler declines an upgrade request, the caller feeds the remainder back to the parser, causing the buffer to grow with each handled request and dispatching already-handled requests to the application again. The issue affects deployments using AIOHTTP_NO_EXTENSIONS or otherwise running without the standard C-extension wheel, and can cause excessive memory use and repeated request processing. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-97845	An uncontrolled recursion vulnerability has been discovered in the Qt QXmlSimpleReader XML parsing functionality of the Qt 5 Core Compatibility APIs module (Qt 6) and the Qt XML module (Qt 5).	N/A	More Details
CVE-2026-126329	Docker Sandboxes reuses existing state and configuration directories without verifying their ownership. If sbx or sandboxd is run as root with HOME or, on Linux, XDG_STATE_HOME pointing to an attacker-controlled location, a local unprivileged user can substitute control-plane sockets and configuration trusted by the root process, potentially executing commands as root. Exploitation requires a privileged invocation with an attacker-influenced environment. The issue affects Linux and macOS and is fixed in version 0.53.0.	N/A	More Details
CVE-2026-126330	Docker Sandboxes can silently republish a sandbox service after an operator removes its automatically assigned host-port mapping. The daemon removes the active binding but retains the original publication request, allowing a later port change or sandbox restart to publish the service again on a new host port. An attacker able to reach the restored endpoint may regain access to the service. Both TCP and UDP mappings are affected. Exposure is limited to the original bind address, which defaults to loopback. The issue is fixed in version 0.53.0.	N/A	More Details
CVE-2026-70641	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority as a duplicate of CVE-2026-82873.	N/A	More Details
CVE-2025-10698	Incorrect default permissions and Product released in Non-Release configuration vulnerability in OpenText Identity Console on Windows, Linux, and 64 bit allows Retrieve Embedded Sensitive Data. This issue affects Identity Console: from 1.8 through 25.2.	N/A	More Details
CVE-2025-53700	CWE-922 Insecure Storage of Sensitive Information vulnerability in Johnson Controls iSTAR Ultra, Johnson Controls iSTAR Ultra SE, Johnson Controls iSTAR Ultra G2, Johnson Controls iSTAR Ultra G2 SE, and Johnson Controls iSTAR Edge G2 allows CAPEC-15 File Manipulation. This issue affects iSTAR Ultra: before 6.9.2.CU02; iSTAR Ultra SE: before 6.9.2.CU02; iSTAR Ultra G2: before 6.9.2.CU02; iSTAR Ultra G2 SE: before 6.9.2.CU02; iSTAR Edge G2: before 6.9.2.CU02.	N/A	More Details
CVE-2025-53699	Missing protection mechanism for alternate hardware interface vulnerability in Johnson Controls iSTAR Ultra, Johnson Controls iSTAR Ultra SE, Johnson Controls iSTAR Ultra G2, Johnson Controls iSTAR Ultra G2 SE, and Johnson Controls iSTAR Edge G2 allows CAPEC-554: Functionality Bypass. This issue affects iSTAR Ultra: before 6.9.2.CU02; iSTAR Ultra SE: before 6.9.2.CU02; iSTAR Ultra G2: before 6.9.2.CU02; iSTAR Ultra G2 SE: before 6.9.2.CU02; iSTAR Edge G2: before 6.9.2.CU02.	N/A	More Details
CVE-2025-53698	Missing protection mechanism for alternate hardware interface vulnerability in Johnson Controls iSTAR Ultra and Johnson Controls iSTAR Ultra SE allows CAPEC-554: Functionality Bypass. This issue affects iSTAR Ultra: before 6.9.2.CU02; iSTAR Ultra SE: before 6.9.2.CU02.	N/A	More Details
CVE-2025-	Use of default credentials vulnerability in Johnson Controls iSTAR Ultra, Johnson Controls iSTAR Ultra SE, Johnson Controls iSTAR Ultra G2, Johnson Controls iSTAR Ultra G2 SE, and Johnson Controls iSTAR Edge G2 allows CAPEC-560: Use of Default Credentials. This issue affects iSTAR Ultra: before 2.9.2.CU02; iSTAR Ultra SE: before	N/A	More Details

53697	6.9.2.CU02; iSTAR Ultra G2: before 6.9.2.CU02; iSTAR Ultra G2 SE: before 6.9.2.CU02; iSTAR Edge G2: before 6.9.2.CU02.		
CVE-2025-43874	: Improper Neutralization of Special Elements used in an OS Command vulnerability in Johnson Controls iSTAR Ultra, Johnson Controls iSTAR Ultra SE, Johnson Controls iSTAR Ultra G2, Johnson Controls iSTAR Ultra G2 SE, and Johnson Controls iSTAR Edge G2 allows : OS Command Injection. This issue affects iSTAR Ultra: before 6.9.2.CU02; iSTAR Ultra SE: before 6.9.2.CU02; iSTAR Ultra G2: before 6.9.2.CU02; iSTAR Ultra G2 SE: before 6.9.2.CU02; iSTAR Edge G2: before 6.9.2.CU02.	N/A	More Details
CVE-2026-126192	Soup Sieve is a CSS selector library designed to be used with Beautiful Soup 4. Prior to 2.10, matching a developer-authored selector that places the general sibling combinator inside :has() repeatedly scans each candidate element's following siblings when the right-hand side is absent, producing quadratic work on attacker-controlled HTML. Applications that evaluate a fixed selector such as div:has(a ~ b) over untrusted markup can have a worker occupied for minutes by a small document, while the adjacent sibling form and trusted-only document processing are not affected in the same way. This issue is fixed in version 2.10.	N/A	More Details
CVE-2026-16052	The http.cookies.Morsel class allows separator semicolons in attribute values and includes them verbatim in all output formats. An attacker who can control these values could use this to relax the cookie's Domain or SameSite restrictions.	N/A	More Details
CVE-2026-82032	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-82977	The Plesk GoAccess statistics integration in Plesk Obsidian for Linux, versions 18.0.77 to 18.0.81.7, 18.0.82 to 18.0.82.2, allows cross-subscription information disclosure.	N/A	More Details
CVE-2026-128133	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-128132	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.4, the WebSocket reader continues parsing frames already received after the receive queue pauses the transport, and empty messages are not counted toward the queue size. With permessage-deflate, one read of compressed frames can add many megabytes of decompressed messages to the receive queue. A remote peer can send many small or compressed messages faster than the application consumes them and cause excessive memory use in a server or client. This issue is fixed in version 3.14.4.	N/A	More Details
CVE-2026-109093	A stack buffer overflow in ProcXTestFakeInput DeviceValuator handling in X.Org xwayland before 24.1.15 and X server before 21.1.26 could be used by authenticated clients to crash or execute code in the X server.	N/A	More Details
CVE-2025-54501	Improper access control on an internal debug interface could allow a high privileged attacker to bypass memory access controls potentially resulting in a loss of SEV-SNP guest memory integrity.	N/A	More Details
CVE-2026-0004	A transient execution vulnerability in some AMD processors may allow an attacker with the ability to execute code on the system to infer data in the L1D cache, potentially resulting in the leakage of sensitive information across privileged boundaries.	N/A	More Details
CVE-2026-0101	Improper validation of specified quantities in input within AMD Power Management Firmware (PMFW) could allow a local attacker to pass unsanitized input, potentially resulting in a system crash or denial of service.	N/A	More Details
CVE-2025-54507	Improper validation of consistency within input in AMD SEV (Secure Encrypted Virtualization) firmware could allow an attacker with administrative privileges to create multiple RMP entries for the same guest physical address, potentially resulting in loss of guest integrity.	N/A	More Details
CVE-2026-97358	An inclusion of web functionality from an untrusted source could allow remote code execution on SpaceCom	N/A	More Details
CVE-2026-97357	An Out-Of-Bounds Write due to missing input validation is possible in the autoprogramming interface of SpaceCom and Space Battery pack with WiFi which could lead to a denial of service of the affected communication device	N/A	More Details
CVE-2026-0455	The Versal™ AI Edge Series Gen 2 Peripheral Protection Unit (XPPU) for the inter-processor interrupt (IPI) buffers does not block unauthorized access as expected. This allows processors in the SoC with any IPI channel access the ability to both read and write to the entire IPI buffer register space as well as the IPI no-buffer register control space.	N/A	More Details
CVE-2026-0460	Improper authentication in Bootgen could result in the use of a fixed salt value for RSA padding instead of a randomly generated salt, potentially impacting data integrity.	N/A	More Details

CVE-2026-126206	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. In 2.25.2, Loofah::HTML5::Scrub.allowed_uri? treats a data URI mediatype containing the HTML5 named solidus reference / as malformed and falls back to the allowed text/plain, while a browser decodes the reference and interprets the same value as text/html. An application that validates a user-controlled URL with this helper and renders the approved value in href or another browser-interpreted URI attribute can allow cross-site scripting. Rails::HTML::Sanitizer.allowed_uri? re-exports the affected helper. Loofah's default sanitize() path is not affected because Nokogiri decodes the entity before URI validation. This issue is fixed in version 2.25.3.	N/A	More Details
CVE-2026-126209	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. From 2.25.0 until 2.25.3, Loofah::HTML5::Scrub.allowed_uri? strips whitespace and control characters before decoding a semicolon-less numeric character reference, changing where the reference ends and hiding a javascript: or vbscript: scheme that a browser reconstructs. The bypass applies to encoded colons and encoded scheme letters when a stripped character terminates the numeric reference. An application that renders the approved value in href or another browser-interpreted URI attribute can allow cross-site scripting, and Rails::HTML::Sanitizer.allowed_uri? re-exports the affected helper. Loofah's default sanitize() path is not affected because Nokogiri decodes entities before URI evaluation. This issue is fixed in version 2.25.3.	N/A	More Details
CVE-2026-120868	Memory overflow in Packet Processing can lead to unpredictable or erroneous behavior or Denial of Service in NetScaler ADC and NetScaler Gateway.	N/A	More Details
CVE-2026-126361	Astro is a web framework for content-driven websites. Prior to 7.4.5, Astro rendered a string used as a dynamic element name as raw HTML after applying an incomplete character filter. A / in the string could make an HTML parser treat the remainder as attributes, allowing untrusted element-name input to inject event-handler markup. The .astro dynamic-tag renderer, JSX renderer, and MDX renderer were affected, and exploitation required an application to use request-controlled or stored untrusted data as all or part of an element name. This issue is fixed in version 7.4.5.	N/A	More Details
CVE-2026-126362	Astro is a web framework for content-driven websites. From 5.7.3 until 9.1.2, the @astrojs/svelte renderer inserted a named slot into the quoted name attribute of an astro-slot wrapper without HTML escaping. Request-controlled slot names containing a quote could terminate the attribute and inject active HTML. Exploitation required a hydrated Svelte component using a client:* directive and dynamic rendering of the attacker-chosen slot; components that did not render that slot emitted only Astro's escaped fallback content. Both server rendering and client-side hydration used the unsafe slot name. This issue is fixed in version 9.1.2.	N/A	More Details
CVE-2026-126363	Astro is a web framework for content-driven websites. From 0.2.0 until 7.1.2, the @astrojs/solid-js renderer inserted a named slot into the quoted name attribute of an astro-slot wrapper without HTML escaping. A request-controlled slot name containing a quote could terminate the attribute and inject active HTML. Exploitation required a hydrated Solid component using a client:* directive and dynamic access to the attacker-chosen slot property; a component that did not render that slot emitted only escaped fallback content. This issue is fixed in version 7.1.2.	N/A	More Details
CVE-2026-126364	Astro is a web framework for content-driven websites. From 5.14.3 until 7.4.7, Astro's /_image endpoint compared the requested local-image path with the build output directory without preserving case on case-sensitive filesystems. A sibling directory whose path differed from the output directory only by letter case could therefore pass the containment check, allowing an unauthenticated requester to read image files accepted by the image service from outside the output directory. Exploitation required on-demand rendering with the @astrojs/node adapter, a case-sensitive filesystem, and a preexisting case-variant sibling directory; ordinary traversal to unrelated paths was already rejected. This issue is fixed in Astro version 7.4.7.	N/A	More Details
CVE-2026-128065	@grpc/grpc-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. From 1.14.0 through 1.14.1, XdsServer in @grpc/grpc-js-xds can acknowledge Route and VirtualHost resources while failing to apply their RBACPerRoute override configurations. The override parser is not registered under the override message type, override maps are stored under a type URL instead of the configured HTTP filter name, and VirtualHost override maps are not read. When experimental RBAC is enabled and a trusted xDS control plane supplies a broad top-level ALLOW policy with a stricter matching override, affected servers evaluate RPCs under the broad policy and can accept requests that should be denied. This issue is fixed in version 1.14.2.	N/A	More Details
CVE-2026-128066	Pillow is a Python imaging library. From 1.0 through 12.3.0, ImageFileDirectory_v2.load() in src/PIL/TiffImagePlugin.py retains a separate bytes object for each out-of-line IFD tag value without limiting the total data read or preventing distinct tags from referencing the same file region. A small crafted TIFF or EXIF-bearing JPEG, PNG, WebP, or MPO can therefore cause memory use quadratic in the input size. TIFF and some JPEG paths trigger parsing during Image.open(), while other formats are exposed when EXIF is requested, including through getexif() or ImageOps.exif_transpose(). The declared pixel dimensions do not bound this metadata allocation, so decompression-bomb checks do not prevent process memory exhaustion. This issue is fixed in version 13.0.0.	N/A	More Details
CVE-2026-	Pillow is a Python imaging library. From 2.3.0 through 12.3.0, Pillow applications that save compressed TIFF images through libtiff can pass attacker-controlled image geometry tags to the encoder while allocating its row buffer from the actual image dimensions. The affected TiffImagePlugin._save path allows ImageWidth, ImageLength, or SamplesPerPixel from exif=, tiffinfo=, or a source TIFF IFD to make libtiff consume a larger scanline than the buffer supplied by ImagingLibTiffEncode. This can read heap memory into the generated TIFF	N/A	More

128067	or crash the process. When TIFF Predictor 2 is enabled, libtiff can rewrite the oversized scanline in place and corrupt memory beyond the buffer. A carried-over PlanarConfiguration value of 2 instead makes libtiff use a shorter scanline and can produce an undecodable output file, but is not established to cause the out-of-bounds access. This issue is fixed in version 13.0.0.		Details
CVE-2026-107407	Memory overflow in SMPP traffic can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-107408	Memory corruption in DNS / DNS-over-HTTPS (DoH) can lead to unpredictable or erroneous behavior or Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-107409	Memory corruption in DNS-over-HTTPS (DoH) can lead to unpredictable or erroneous behavior or a Denial of Service in Citrix NetScaler	N/A	More Details
CVE-2026-97361	There exists an improper privilege management vulnerability that could cause privilege escalation at the SpaceCom and Space Battery pack SP with WiFi.	N/A	More Details
CVE-2026-102537	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to versions 1.4.6, 1.5.2, and 1.6.1, bws_cli_connect() in ports/linux/websocket-cli.c loads the trusted CA cert into the libwebsockets context, then always sets LCCSCF_ALLOW_SELFSIGNED in the connection flags. So lws accepts any self-signed hub certificate, whether or not it chains to the loaded CA. A BACnet/SC node finishes the TLS handshake to a rogue hub that presents a self-signed cert. It then hands the attacker its identity (VMAC, UUID) and all later BACnet traffic. This issue has been patched in versions 1.4.6, 1.5.2, 1.6.1, and 1.7.0.	N/A	More Details
CVE-2026-0436	Insufficient parameter sanitization in the AMD Secure Processor (ASP) trusted execution environment (TEE) SPDM driver could allow an attacker to supply malicious input, potentially resulting in loss of platform integrity, memory leakage, or denial of service.	N/A	More Details
CVE-2025-0043	Incorrect directory permissions within AMD Vivado™ Lab Solutions could allow a local user-privileged attacker to escalate their privileges, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2026-68541	PolicyPress is a compliance policy management tool for small and mid-size teams. Prior to version 1.4.1, sensitive content is disclosed via CSS-only web redaction and insecure starter workflow defaults. This issue has been patched in version 1.4.1.	N/A	More Details
CVE-2026-68510	bit-vec is a compact vector of bits. Prior to version 0.10.0, there is undefined behavior if a user performs deserialize from an untrusted source and unsafe get_unchecked. A user of this library may be impacted by incorrect behavior if they perform deserialize from an untrusted source and run operations on the deserialized BitVec. This issue has been patched in version 0.10.0.	N/A	More Details
CVE-2026-67444	Hubleys is a dashboard for self-hosted services. Prior to version 0.5.2, any authenticated (non-admin) Hubleys user can upload a file with an arbitrary extension as their dashboard "background image," and the server will later serve that file back with a Content-Type derived straight from the attacker's chosen extension - so uploading an .html file gets it served as text/html. Because the endpoint that serves it returns a manually-constructed response rather than going through SvelteKit's normal page-rendering pipeline, the app's configured Content-Security-Policy never gets attached to it either, so a script embedded in the upload runs unrestricted. This issue has been patched in version 0.5.2.	N/A	More Details
CVE-2026-117542	Joomla Extension - jdownloads.com - Authenticated path traversal in jDownloads < 4.1.8 - A manipulated `update_file` form parameter could bypass the intended server-file selection restrictions and move files from outside the permitted selection directory or assign them to a download. This could expose file contents and remove source files from their original locations.	N/A	More Details
CVE-2026-62977	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to version 1.5.1, the BACnet FILE object implementation allows remote WriteProperty(PROP_FILE_SIZE) requests to change the size of a stream-access FILE object without checking whether that FILE is marked Read_Only. When the FILE backend is RAMFS, enlarging the file only performs realloc() and updates the stored size; the newly exposed tail region is not initialized before later reads. As a result, a remote client can enlarge a read-only RAMFS-backed stream-access FILE and then immediately retrieve the newly exposed region with AtomicReadFile(stream-access). Depending on the allocator and build configuration, the returned data may contain sanitizer fill bytes, stale heap contents, or other unintended process memory. Shrinking the file through the same path can also remotely truncate content that was intended to be read-only. This issue has been patched in versions 1.5.1 and 1.6.0.	N/A	More Details
CVE-2026-62976	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to version 1.5.1, the RAMFS-backed FILE object implementation stores appended records as NUL-terminated strings, but its record-counting logic later walks the buffer as if an additional terminating empty record were present. As a result, two consecutive AtomicWriteFile(record-access) append requests can cause record_count() to call bacnet_strnlen() on a pointer that is already one byte past the end of the heap allocation. This issue has been patched in versions 1.5.1 and 1.6.0.	N/A	More Details

CVE-2026-62975	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to version 1.5.1, the RAMFS-backed FILE implementation accepts AtomicWriteFile(record-access) requests that replace existing records with caller-controlled content. If a client replaces a record with shorter data, the backend can shrink the heap allocation and then continue processing with a trailing-copy length derived from the old layout. During that replace path, the RAMFS backend computes the trailing-copy length from the old file layout, then shrinks the heap allocation, and finally uses the stale length in memmove(). As a result, the source range of that memmove() can extend beyond the end of the reallocated heap buffer, producing a heap out-of-bounds read. This issue has been patched in versions 1.5.1 and 1.6.0.	N/A	More Details
CVE-2026-43626	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority, replacedby CVE-2026-70640.	N/A	More Details
CVE-2026-129217	In FRRouting (FRR) 8.3 through 10.5.1, bgp_notify_decapsulate_hard_reset() in bgpd/bgp_packet.c does not validate the length of the data field of a received BGP NOTIFICATION Cease/Hard Reset message (RFC 8538). When the data field is exactly one byte long, the function reads one byte past the end of a heap buffer and the 16-bit length of the encapsulated data underflows to 65535, causing a 65535-byte out-of-bounds heap read followed by an assertion failure. A remote BGP peer that has established a session and negotiated the Graceful Restart capability with the Notification (N) bit can send such a message to crash the bgpd daemon, terminating all BGP sessions (denial of service). This is fixed in 10.0.5, 10.1.5, 10.2.6, 10.3.4, 10.4.3, 10.5.2 and 10.6.0.	N/A	More Details
CVE-2026-117544	Joomla Extension - jdownloads.com - IDOR allowing restricted file downloads in jDownloads < 4.1.8 - The `other_file_id` parameter could reference another download’s file without fully enforcing the target download’s access restrictions. This allowed files to be delivered to users who were not authorised to access the target download.	N/A	More Details
CVE-2026-120033	In FRRouting, bgpd does not correctly close a BGP session when the Send Hold Timer (RFC 9687) expires, i.e. when a neighbor has stopped accepting data from the router for twice the hold time. The connection is closed, but bgpd still considers the session to be up. A BGP neighbor that keeps sending KEEPALIVEs but stops reading from its connection, at a time when the router has a large amount of data to send to it (for example while sending it a full routing table), can trigger this. If the neighbor announced Graceful Restart support, bgpd crashes shortly after the session is closed, taking down all BGP sessions on the router, and the neighbor can repeat this each time bgpd restarts. Otherwise, the session stays stuck in the Established state: the neighbor's routes stay installed and keep being advertised to other peers, and the neighbor cannot reconnect until an operator clears the session manually. The neighbor does not need to be malicious; an overloaded or stuck peer can trigger the same behavior. No special configuration is required: any established BGP neighbor can trigger the issue, and Graceful Restart helper mode, which leads to the crash, is enabled by default.	N/A	More Details
CVE-2026-120467	Joomla / WordPress Extension - acymailing.com - Subscriber identity not bound to the record acted upon in AcyMailing 1.0.0 - 11.1.1 - An authenticated user of any privilege level can subscribe or unsubscribe any other subscriber to or from any mailing list of the site.	N/A	More Details
CVE-2026-121619	The Symfony FrameworkBundle framework.trusted_proxies option and the HttpFoundation Request::setTrustedProxies() method trust remote clients as reverse proxies when the private_ranges shortcut is used, allowing remote attackers to spoof the client IP address, host and scheme in Symfony FrameworkBundle versions 7.1 prior to 7.4.23 and 8.x prior to 8.1.11, and HttpFoundation versions 7.2 prior to 7.4.23 and 8.x prior to 8.1.11. The private_ranges and PRIVATE_SUBNETS keywords resolved to IpUtils::PRIVATE_SUBNETS, the deny list of NoPrivateNetworkHttpClient, which lists the private and special-purpose prefixes a server must not connect to. Since the fix for CVE-2026-48736 (7.4.13 and 8.0.13), this list also covers the IPv6 prefixes that embed an IPv4 address: IPv4-mapped (::ffff:0:0/96), IPv4-compatible (::/96), 6to4 (2002::/16), Teredo (2001::/32) and NAT64 (64:ff9b::/96). The IPv4-mapped entry has been in the list since the private_ranges shortcut was introduced, in 7.1 for framework.trusted_proxies and in 7.2 for Request::setTrustedProxies(). Over-blocking is safe for a deny list, but when the same entries are used as the allow list of trusted proxies, they trust remote clients. A client whose connection arrives with such a source address is treated as a reverse proxy, and the X-Forwarded-For, X-Forwarded-Host, X-Forwarded-Proto, X-Forwarded-Port and X-Forwarded-Prefix headers it sends are honoured. For example, with Request::setTrustedProxies(['private_ranges'], ...), a request with REMOTE_ADDR set to ::ffff:203.0.113.7 and the headers X-Forwarded-For: 10.0.0.9, X-Forwarded-Host: evil.example.com and X-Forwarded-Proto: https makes getClientIp() return 10.0.0.9, getHost() return evil.example.com and isSecure() return true. Two kinds of deployments are exposed: a server listening on the IPv6 wildcard address without IPV6_V6ONLY reports every IPv4 client in the IPv4-mapped form, so every client is trusted, and a server reachable over IPv6 trusts any client sourcing from 6to4 or Teredo space, which is globally routed, whatever its listener. A spoofed client address defeats IP allow lists, rate limiting and audit logs; a spoofed host poisons the URLs written into password reset and login link e-mails and into shared caches; a spoofed scheme satisfies requires_channel: https over plain HTTP. Symfony 6.4 does not point any trusted proxy setting at IpUtils::PRIVATE_SUBNETS and is not affected by default, but an application that passes that constant to Request::setTrustedProxies() itself could be exposed in the same way on any version. This issue is fixed in 7.4.23 and 8.1.11.	N/A	More Details
CVE-2026-	Laravel is a web application framework. Prior to 12.71.0 and 13.40.0, Laravel's Concurrency::run process driver can treat a forged internal result message in child standard output as framework output. An application route must invoke Concurrency::run, and a task must write attacker-controlled bytes at the start of the child's standard output that form a complete JSON document followed by gzip magic bytes. Under those application-	N/A	More

128083	specific conditions, an attacker can forge the internal result message and achieve remote code execution. The affected behavior is not exposed by default and requires application code that routes untrusted input into task output. This issue is fixed in versions 12.71.0 and 13.40.0.		Details
CVE-2024-21963	An out-of-bounds read vulnerability in the IOMMU could allow a malicious guest to corrupt hypervisor (HV) pages and potentially cause a host crash leading to loss of availability.	N/A	More Details
CVE-2024-36344	Insufficient parameter sanitization in AMD Secure Processor (ASP) TEE DrvSys could allow an attacker with local access to the Trusted Execution Environment (TEE) interface or Trusted Application (TA) to cause an out-of-bounds write, potentially resulting in a loss of platform integrity or denial of service.	N/A	More Details
CVE-2026-104204	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to version 1.6.1, there is a server-side denial-of-service issue affecting the Structured View object implementation. This issue has been patched in versions 1.6.1 and 1.7.0.	N/A	More Details
CVE-2026-106018	Authentication bypass using an alternate path or channel vulnerability in Johnson Controls EasyIO FW allows Authentication Bypass. This issue affects EasyIO FW: through 3.0b25.	N/A	More Details