SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 February 2026

Generated on 25 February 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-2026-23693	ElementsKit Elementor Addons – Advanced Widgets & Templates Addons for Elementor (elementskit-lite) WordPress plugin versions prior to 3.7.9 expose the REST endpoint /wp-json/elementskit/v1/widget/mailchimp/subscribe without authentication. The endpoint accepts client-supplied Mailchimp API credentials and insufficiently validates certain parameters, including the list parameter, when constructing upstream Mailchimp API requests. An unauthenticated attacker can abuse the endpoint as an open proxy to Mailchimp, potentially triggering unauthorized API calls, manipulating subscription data, exhausting API quotas, or causing resource consumption on the affected WordPress site.	10.0	More Details
CVE-2021-35402	PROLiNK PRC2402M 20190909 before 2021-06-13 allows live_api.cgi?page=satellite_list OS command injection via shell metacharacters in the ip parameter (for satellite_status).	10.0	More Details
CVE-2026-27211	Cloud Hypervisor is a Virtual Machine Monitor for Cloud workloads. Versions 34.0 through 50.0 arevulnerable to arbitrary host file exfiltration (constrained by process privileges) when using virtio-block devices backed by raw images. A malicious guest can overwrite its disk header with a crafted QCOW2 structure pointing to a sensitive host path. Upon the next VM boot or disk scan, the image format auto-detection parses this header and serves the host file's contents to the guest. Guest-initiated VM reboots are sufficient to trigger a disk scan and do not cause the Cloud Hypervisor process to exit. Therefore, a single VM can perform this attack without needing interaction from the management stack. Successful exploitation requires the backing image to be either writable by the guest or sourced from an untrusted origin. Deployments utilizing only trusted, read-only images are not affected. This issue has been fixed in version 50.1. To workaround, enable land lock sandboxing and restrict process privileges and access.	10.0	More Details
CVE-2025-12107	Due to the use of a vulnerable third-party Velocity template engine, a malicious actor with admin privilege may inject and execute arbitrary template syntax within server-side templates. Successful exploitation of this vulnerability could allow a malicious actor with admin privilege to inject and execute arbitrary template code on the server, potentially leading to remote code execution, data manipulation, or unauthorized access to sensitive information.	10.0	More Details
CVE-2026-26030	Semantic Kernel, Microsoft's semantic kernel Python SDK, has a remote code execution vulnerability in versions prior to 1.39.4, specifically within the `InMemoryVectorStore` filter functionality. The problem has been fixed in version `python-1.39.4`. Users should upgrade this version or higher. As a workaround, avoid using `InMemoryVectorStore` for production scenarios.	9.9	More Details
CVE-2026-27574	OneUptime is a solution for monitoring and managing online services. In versions 9.5.13 and below, custom JavaScript monitor feature uses Node.js's node:vm module (explicitly documented as not a security mechanism) to execute user-supplied code, allowing trivial sandbox escape via a well-known one-liner that grants full access to the underlying process. Because the probe runs with host networking and holds all cluster credentials (ONEUPTIME_SECRET, DATABASE_PASSWORD, REDIS_PASSWORD, CLICKHOUSE_PASSWORD) in its environment variables, and monitor creation is available to the lowest role (ProjectMember) with open registration enabled by default, any anonymous user can achieve full cluster compromise in about 30 seconds. This issue has been fixed in version 10.0.5.	9.9	More Details
CVE-2026-1937	The YayMail – WooCommerce Email Customizer plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the `yaymail_import_state` AJAX action in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	9.8	More Details

CVE-2025-67997	Deserialization of Untrusted Data vulnerability in BoldThemes Travelicious travelicious allows Object Injection.This issue affects Travelicious: from n/a through < 1.6.7.	9.8	More Details
CVE-2025-69371	Deserialization of Untrusted Data vulnerability in AncoraThemes KindlyCare kindlycare allows Object Injection.This issue affects KindlyCare: from n/a through <= 1.6.1.	9.8	More Details
CVE-2025-69370	Deserialization of Untrusted Data vulnerability in ThemeGoods Capella capella allows Object Injection.This issue affects Capella: from n/a through <= 2.5.5.	9.8	More Details
CVE-2025-69329	Deserialization of Untrusted Data vulnerability in Jthemes Prestige prestige allows Object Injection.This issue affects Prestige: from n/a through < 1.4.1.	9.8	More Details
CVE-2026-1435	Not properly invalidated session vulnerability in Graylog Web Interface, version 2.2.3, due to incorrect management of session invalidation after new logins. The application generates a new 'sessionId' each time a user authenticates, but does not invalidate previously issued session identifiers, which remain valid even after multiple consecutive logins by the same user. As a result, a stolen or leaked 'sessionId' can continue to be used to authenticate valid requests. Exploiting this vulnerability would allow an attacker with access to the web service/API network (port 9000 or HTTP/S endpoint of the server) to reuse an old session token to gain unauthorized access to the application, interact with the API/web, and compromise the integrity of the affected account.	9.8	More Details
CVE-2025-68541	Deserialization of Untrusted Data vulnerability in BoldThemes Ippsum ippsum allows Object Injection.This issue affects Ippsum: from n/a through <= 1.2.0.	9.8	More Details
CVE-2025-67996	Deserialization of Untrusted Data vulnerability in BoldThemes Nestin nestin allows Object Injection.This issue affects Nestin: from n/a through < 1.2.6.	9.8	More Details
CVE-2025-69382	Deserialization of Untrusted Data vulnerability in themesflat Themesflat Elementor themesflat-elementor allows Object Injection.This issue affects Themesflat Elementor: from n/a through <= 1.0.1.	9.8	More Details
CVE-2025-67995	Deserialization of Untrusted Data vulnerability in LoftOcean PatioTime patiotime allows Object Injection.This issue affects PatioTime: from n/a through < 2.1.	9.8	More Details
CVE-2025-10970	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Kolay Software Inc. Talentics allows Blind SQL Injection.This issue affects Talentics: through 20022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-27002	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a configuration injection issue in the Docker tool sandbox could allow dangerous Docker options (bind mounts, host networking, unconfined profiles) to be applied, enabling container escape or host data access. OpenClaw 2026.2.15 blocks dangerous sandbox Docker settings and includes runtime enforcement when building `docker create` args; config-schema validation for `network=host`, `seccompProfile=unconfined`, `apparmorProfile=unconfined`; and security audit findings to surface dangerous sandbox docker config. As a workaround, do not configure `agents.*.sandbox.docker.binds` to mount system directories or Docker socket paths, keep `agents.*.sandbox.docker.network` at `none` (default) or `bridge`, and do not use `unconfined` for seccomp/AppArmor profiles.	9.8	More Details
CVE-2026-27476	RustFly 2.0.0 contains a command injection vulnerability in its remote UI control mechanism that accepts hex-encoded instructions over UDP port 5005 without proper sanitization. Attackers can send crafted hex-encoded payloads containing system commands to execute arbitrary operations on the target system, including reverse shell establishment and command execution.	9.8	More Details
CVE-2025-67305	In RUCKUS Network Director (RND) < 4.5.0.56, the OVA appliance contains hardcoded SSH keys for the postgres user. These keys are identical across all deployments, allowing an attacker with network access to authenticate via SSH without a password. Once authenticated, the attacker can access the PostgreSQL database with superuser privileges, create administrative users for the web interface, and potentially escalate privileges further.	9.8	More Details
CVE-2025-67304	In Ruckus Network Director (RND) < 4.5.0.54, the OVA appliance contains hardcoded credentials for the ruckus PostgreSQL database user. In the default configuration, the PostgreSQL service is accessible over the network on TCP port 5432. An attacker can use the hardcoded credentials to authenticate remotely, gaining superuser access to the database. This allows creation of administrative users for the web interface, extraction of password hashes, and execution of arbitrary OS commands.	9.8	More Details
CVE-2025-69372	Deserialization of Untrusted Data vulnerability in AncoraThemes SevenHills sevenhills allows Object Injection.This issue affects SevenHills: from n/a through <= 1.6.2.	9.8	More Details
CVE-2025-70831	A Remote Code Execution (RCE) vulnerability was found in Smanga 3.2.7 in the /php/path/rescan.php interface. The application fails to properly sanitize user-supplied input in the mediaId parameter before using it in a system shell command. This allows an unauthenticated attacker to inject arbitrary operating system commands, leading to complete server compromise.	9.8	More Details
CVE-2025-69404	Deserialization of Untrusted Data vulnerability in ThemeREX Extreme Store extremestore allows Object Injection.This issue affects Extreme Store: from n/a through <= 1.5.7.	9.8	More Details
CVE-2025-69405	Deserialization of Untrusted Data vulnerability in ThemeREX Lorem Ipsum | Books & Media Store lorem-ipsum-books-media-store allows Object Injection.This issue affects Lorem Ipsum | Books & Media Store: from n/a through <= 1.2.6.	9.8	More Details
CVE-2026-22365	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Soleng soleng allows PHP Local File Inclusion.This issue affects Soleng: from n/a through <= 1.0.5.	9.8	More Details
CVE-2026-25715	The web management interface of the device allows the administrator username and password to be set to blank values. Once applied, the device permits authentication with empty credentials over the web management interface and Telnet service. This effectively disables authentication across all critical management channels, allowing any network-adjacent attacker to gain full administrative control without credentials.	9.8	More Details

CVE-2026-26725	An issue in edu Business Solutions Print Shop Pro WebDesk v.18.34 allows a remote attacker to escalate privileges via the AccessID parameter.	9.8	More Details
CVE-2019-25441	thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint. Attackers can send POST requests with shell commands in the command parameter to execute arbitrary code on the server without authentication.	9.8	More Details
CVE-2026-2038	GFI Archiver MArc.Core Missing Authorization Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the MArc.Core.Remoting.exe process, which listens on port 8017. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of SYSTEM. Was ZDI-CAN-27934.	9.8	More Details
CVE-2026-2039	GFI Archiver MArc.Store Missing Authorization Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the MArc.Store.Remoting.exe process, which listens on port 8018. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of SYSTEM. Was ZDI-CAN-28597.	9.8	More Details
CVE-2026-27194	D-Tale is a visualizer for pandas data structures. Versions prior to 3.20.0 are vulnerable to Remote Code Execution through the /save-column-filter endpoint. Users hosting D-Tale publicly can be vulnerable to remote code execution allowing attackers to run malicious code on the server. This issue has been fixed in version 3.20.0.	9.8	More Details
CVE-2026-24494	SQL Injection vulnerability in the /api/integrations/getintegrations endpoint of Order Up Online Ordering System 1.0 allows an unauthenticated attacker to access sensitive backend database data via a crafted store_id parameter in a POST request.	9.8	More Details
CVE-2025-13942	A command injection vulnerability in the UPnP function of the Zyxel EX3510-B0 firmware versions through 5.17(ABUP.15.1)C0 could allow a remote attacker to execute operating system (OS) commands on an affected device by sending specially crafted UPnP SOAP requests.	9.8	More Details
CVE-2026-26198	Ormar is a async mini ORM for Python. In versions 0.9.9 through 0.22.0, when performing aggregate queries, Ormar ORM constructs SQL expressions by passing user-supplied column names directly into `sqlalchemy.text()` without any validation or sanitization. The `min()` and `max()` methods in the `QuerySet` class accept arbitrary string input as the column parameter. While `sum()` and `avg()` are partially protected by an `is_numeric` type check that rejects non-existent fields, `min()` and `max()` skip this validation entirely. As a result, an attacker-controlled string is embedded as raw SQL inside the aggregate function call. Any unauthorized user can exploit this vulnerability to read the entire database contents, including tables unrelated to the queried model, by injecting a subquery as the column parameter. Version 0.23.0 contains a patch.	9.8	More Details
CVE-2026-27507	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior contain hard-coded administrative credentials that cannot be changed by users. Knowledge of these credentials allows full administrative access to the device.	9.8	More Details
CVE-2026-21410	InSAT MasterSCADA BUK-TS is susceptible to SQL Injection through its main web interface. Malicious users that use the vulnerable endpoint are potentially able to cause remote code execution.	9.8	More Details
CVE-2026-22553	All versions of InSAT MasterSCADA BUK-TS are susceptible to OS command injection through a field in its MMadmServ web interface. Malicious users that use the vulnerable endpoint are potentially able to cause remote code execution.	9.8	More Details
CVE-2026-26339	Hyland Alfresco Transformation Service allows unauthenticated attackers to achieve remote code execution through the argument injection vulnerability, which exists in the document processing functionality.	9.8	More Details
CVE-2025-69301	Deserialization of Untrusted Data vulnerability in ThemeGoods PhotoMe photome allows Object Injection.This issue affects PhotoMe: from n/a through <= 5.6.11.	9.8	More Details
CVE-2019-25360	Aida64 Engineer 6.10.5200 contains a buffer overflow vulnerability in the CSV logging configuration that allows attackers to execute malicious code by crafting a specially designed payload. Attackers can exploit the vulnerability by creating a malformed log file with carefully constructed SEH (Structured Exception Handler) overwrite techniques to achieve remote code execution.	9.8	More Details
CVE-2026-2686	A security vulnerability has been detected in SECCN Dingcheng G10 3.1.0.181203. This impacts the function qq of the file /cgi-bin/session_login.cgi. The manipulation of the argument User leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2025-13563	The Lizza LMS Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'lizza_lms_pro_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-13851	The Buyent Classified plugin for WordPress (bundled with Buyent theme) is vulnerable to privilege escalation via user registration in all versions up to, and including, 1.0.7. This is due to the plugin not validating or restricting the user role during registration via the REST API endpoint. This makes it possible for unauthenticated attackers to register accounts with arbitrary roles, including administrator, by manipulating the _buyent_classified_user_type parameter during the registration process, granting them complete control over the WordPress site.	9.8	More Details
CVE-2026-0926	The Prodigy Commerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.9 via the 'parameters[template_name]' parameter. This makes it possible for unauthenticated attackers to include and read arbitrary files or execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	9.8	More Details

CVE-2026-1405	The Slider Future plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'slider_future_handle_image_upload' function in all versions up to, and including, 1.0.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2026-27174	MajorDoMo (aka Major Domestic Module) allows unauthenticated remote code execution via the admin panel's PHP console feature. An include order bug in modules/panel.class.php causes execution to continue past a redirect() call that lacks an exit statement, allowing unauthenticated requests to reach the ajax handler in inc_panel_ajax.php. The console handler within that file passes user-supplied input from GET parameters (via register_globals) directly to eval() without any authentication check. An attacker can execute arbitrary PHP code by sending a crafted GET request to /admin.php with ajax_panel, op, and command parameters.	9.8	More Details
CVE-2019-25365	ChaosPro 2.0 contains a buffer overflow vulnerability in the configuration file path handling that allows attackers to execute arbitrary code by overwriting the Structured Exception Handler. Attackers can craft a malicious configuration file with carefully constructed payload to overwrite memory and gain remote code execution on vulnerable Windows XP systems.	9.8	More Details
CVE-2026-1994	The s2Member plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 260127. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	9.8	More Details
CVE-2019-25364	MailCarrier 2.51 contains a buffer overflow vulnerability in the POP3 USER command that allows remote attackers to execute arbitrary code. Attackers can send a crafted oversized buffer to the POP3 service, overwriting memory and potentially gaining remote system access.	9.8	More Details
CVE-2019-25362	WMV to AVI MPEG DVD WMV Convertor 4.6.1217 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the license name and license code fields. Attackers can craft a malicious payload of 6000 bytes to trigger a bind shell on port 4444 by exploiting a stack-based buffer overflow in the application's input handling.	9.8	More Details
CVE-2019-25361	Ayukov NFTP client 1.71 contains a buffer overflow vulnerability in the SYST command handling that allows remote attackers to execute arbitrary code. Attackers can send a specially crafted SYST command with oversized payload to trigger a buffer overflow and execute a bind shell on port 5150.	9.8	More Details
CVE-2026-27175	MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated OS command injection via rc/index.php. The $param variable from user input is interpolated into a command string within double quotes without sanitization via escapeshellarg(). The command is inserted into a database queue by safe_exec(), which performs no sanitization. The cycle_execs.php script, which is web-accessible without authentication, retrieves queued commands and passes them directly to exec(). An attacker can exploit a race condition by first triggering cycle_execs.php (which purges the queue and enters a polling loop), then injecting a malicious command via the rc endpoint while the worker is polling. The injected shell metacharacters expand inside double quotes, achieving remote code execution within one second.	9.8	More Details
CVE-2025-70152	code-projects Community Project Scholars Tracking System 1.0 is vulnerable to SQL Injection in the admin user management endpoints /admin/save_user.php and /admin/update_user.php. These endpoints lack authentication checks and directly concatenate user-supplied POST parameters (firstname, lastname, username, password, user_id) into SQL queries without validation or parameterization.	9.8	More Details
CVE-2025-70150	CodeAstro Membership Management System 1.0 contains a missing authentication vulnerability in delete_members.php that allows unauthenticated attackers to delete arbitrary member records via the id parameter.	9.8	More Details
CVE-2025-70149	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in print_membership_card.php via the ID parameter.	9.8	More Details
CVE-2026-25242	Gogs is an open source self-hosted Git service. Versions 0.13.4 and below expose unauthenticated file upload endpoints by default. When the global RequireSigninView setting is disabled (default), any remote user can upload arbitrary files to the server via /releases/attachments and /issues/attachments. This enables the instance to be abused as a public file host, potentially leading to disk exhaustion, content hosting, or delivery of malware. CSRF tokens do not mitigate this attack due to same-origin cookie issuance. This issue has been fixed in version 0.14.1.	9.8	More Details
CVE-2026-27180	MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated remote code execution through supply chain compromise via update URL poisoning. The saverestore module exposes its admin() method through the /objects/?module=saverestore endpoint without authentication because it uses gr('mode') (which reads directly from $_REQUEST) instead of the framework's $this->mode. An attacker can poison the system update URL via the auto_update_settings mode handler, then trigger the force_update handler to initiate the update chain. The autoUpdateSystem() method fetches an Atom feed from the attacker-controlled URL with trivial validation, downloads a tarball via curl with TLS verification disabled (CURLOPT_SSL_VERIFYPEER set to FALSE), extracts it using exec('tar xzvf ...'), and copies all extracted files to the document root using copyTree(). This allows an attacker to deploy arbitrary PHP files, including webshells, to the webroot with two GET requests.	9.8	More Details
CVE-2026-23542	Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Restaurant grandrestaurant allows Object Injection.This issue affects Grand Restaurant: from n/a through <= 7.0.10.	9.8	More Details
CVE-2026-23549	Deserialization of Untrusted Data vulnerability in magepeopleteam WpEvently mage-eventpress allows Object Injection.This issue affects WpEvently: from n/a through <= 5.1.1.	9.8	More Details
CVE-2025-70998	UTT HiPER 810 / nv810v4 router firmware v1.5.0-140603 was discovered to contain insecure default credentials for the telnet service, possibly allowing a remote attacker to gain root access via a crafted script.	9.8	More Details
CVE-2025-15559	An unauthenticated attacker can inject OS commands when calling a server API endpoint in NesterSoft WorkTime. The server API call to generate and download the WorkTime client from the WorkTime server is vulnerable in the “guid” parameter. This allows an attacker to execute arbitrary commands on the WorkTime server as NT Authority\SYSTEM	9.8	More Details

	with the highest privileges. Attackers are able to access or manipulate sensitive data and take over the whole server.		
CVE-2025-8350	Execution After Redirect (EAR), Missing Authentication for Critical Function vulnerability in Inrove Software and Internet Services BiEticaret CMS allows Authentication Bypass, HTTP Response Splitting.This issue affects BiEticaret CMS: from 2.1.13 through 19022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-65791	ZoneMinder v1.36.34 is vulnerable to Command Injection in web/views/image.php. The application passes unsanitized user input directly to the exec() function.	9.8	More Details
CVE-2025-69674	Buffer Overflow vulnerability in CDATA FD614GS3-R850 V3.2.7_P161006 (Build.0333.250211) allows an attacker to execute arbitrary code via the node_mac, node_opt, opt_param, and domainblk parameters of the mesh_node_config and domiainblk_config modules	9.8	More Details
CVE-2025-9953	Authorization Bypass Through User-Controlled SQL Primary Key vulnerability in DATABASE Software Training Consulting Ltd. Databank Accreditation Software allows SQL Injection.This issue affects Databank Accreditation Software: through 19022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-2329	An unauthenticated stack-based buffer overflow vulnerability exists in the HTTP API endpoint /cgi-bin/api.values.get. A remote attacker can leverage this vulnerability to achieve unauthenticated remote code execution (RCE) with root privileges on a target device. The vulnerability affects all six device models in the series: GXP1610, GXP1615, GXP1620, GXP1625, GXP1628, and GXP1630.	9.8	More Details
CVE-2025-71243	The 'Saisies pour formulaire' (Saisies) plugin for SPIP versions 5.4.0 through 5.11.0 contains a critical Remote Code Execution (RCE) vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the server. Users should immediately update to version 5.11.1 or later.	9.8	More Details
CVE-2025-12882	The Clasifico Listing plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.0. This is due to the plugin allowing users who are registering new accounts to set their own role by supplying the 'listing_user_role' parameter. This makes it possible for unauthenticated attackers to gain elevated privileges by registering an account with the administrator role.	9.8	More Details
CVE-2026-26722	An issue in Key Systems Inc Global Facilities Management Software v.20230721a allows a remote attacker to escalate privileges via PIN component of the login functionality.	9.4	More Details
CVE-2025-70833	An Authentication Bypass vulnerability in Smanga 3.2.7 allows an unauthenticated attacker to reset the password of any user (including the administrator) and fully takeover the account by manipulating POST parameters. The issue stems from insecure permission validation in check-power.php.	9.4	More Details
CVE-2025-70141	SourceCodester Customer Support System 1.0 contains an incorrect access control vulnerability in ajax.php. The AJAX dispatcher does not enforce authentication or authorization before invoking administrative methods in admin_class.php based on the action parameter. An unauthenticated remote attacker can perform sensitive operations such as creating customers and deleting users (including the admin account), as well as modifying or deleting other application records (tickets, departments, comments), resulting in unauthorized data modification.	9.4	More Details
CVE-2026-26980	Ghost is a Node.js content management system. Versions 3.24.0 through 6.19.0 allow unauthenticated attackers to perform arbitrary reads from the database. This issue has been fixed in version 6.19.1.	9.4	More Details
CVE-2026-25896	fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. From 4.1.3to before 5.3.5, a dot (.) in a DOCTYPE entity name is treated as a regex wildcard during entity replacement, allowing an attacker to shadow built-in XML entities (<, >, &, ", ') with arbitrary values. This bypasses entity encoding and leads to XSS when parsed output is rendered. This vulnerability is fixed in 5.3.5.	9.3	More Details
CVE-2026-24834	Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. In versions prior to 3.27.0, an issue in Kata with Cloud Hypervisor allows a user of the container to modify the file system used by the Guest micro VM ultimately achieving arbitrary code execution as root in said VM. The current understanding is this doesn’t impact the security of the Host or of other containers / VMs running on that Host (note that arm64 QEMU lacks NVDIMM read-only support: It is believed that until the upstream QEMU gains this capability, a guest write could reach the image file). Version 3.27.0 patches the issue.	9.3	More Details
CVE-2026-24956	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shahjada Download Manager Addons for Elementor wpdm-elementor allows Blind SQL Injection.This issue affects Download Manager Addons for Elementor: from n/a through <= 1.3.0.	9.3	More Details
CVE-2026-27593	Statmatic is a Laravel and Git powered content management system (CMS). Prior to versions 6.3.3 and 5.73.10, an attacker may leverage a vulnerability in the password reset feature to capture a user's token and reset the password on their behalf. The attacker must know the email address of a valid account on the site, and the actual user must blindly click the link in their email even though they didn't request the reset. This has been fixed in 6.3.3 and 5.73.10.	9.3	More Details
CVE-2025-69308	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Nestbyte Core nestbyte-core allows Blind SQL Injection.This issue affects Nestbyte Core: from n/a through <= 1.2.	9.3	More Details
CVE-2025-69304	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Allmart allmart-core allows Blind SQL Injection.This issue affects Allmart: from n/a through <= 1.1.	9.3	More Details
CVE-2025-69366	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Emerce Core emerce-core allows Blind SQL Injection.This issue affects Emerce Core: from n/a through <= 1.8.	9.3	More Details
CVE-2025-69305	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Crete Core crete-core allows Blind SQL Injection.This issue affects Crete Core: from n/a through <= 1.4.3.	9.3	More Details
CVE-2025-69306	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Electio Core electio-core allows Blind SQL Injection.This issue affects Electio Core: from n/a through <= 1.4.	9.3	More Details

CVE-2025-69307	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Medinik Core medinik-core allows Blind SQL Injection.This issue affects Medinik Core: from n/a through <= 1.3.6.	9.3	More Details
CVE-2025-69295	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Coven Core coven-core allows Blind SQL Injection.This issue affects Coven Core: from n/a through <= 1.3.	9.3	More Details
CVE-2025-69309	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Saasplate Core saasplate-core allows Blind SQL Injection.This issue affects Saasplate Core: from n/a through <= 1.2.8.	9.3	More Details
CVE-2025-69310	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Woodly Core woodly-core allows Blind SQL Injection.This issue affects Woodly Core: from n/a through <= 1.4.	9.3	More Details
CVE-2025-69337	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in don-themes Wolmart Core wolmart-core allows Blind SQL Injection.This issue affects Wolmart Core: from n/a through <= 1.9.6.	9.3	More Details
CVE-2025-69365	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeconceTheme Uroan Core uroan-core allows Blind SQL Injection.This issue affects Uroan Core: from n/a through <= 1.4.4.	9.3	More Details
CVE-2026-27208	bleon-ethical/api-gateway-deploy provides API gateway deployment. Version 1.0.0 is vulnerable to an attack chain involving OS Command Injection and Privilege Escalation. This allows an attacker to execute arbitrary commands with root privileges within the container, potentially leading to a container escape and unauthorized infrastructure modifications. This is fixed in version 1.0.1 by implementing strict input sanitization and secure delimiters in entrypoint.sh, enforcing a non-root user (appuser) in the Dockerfile, and establishing mandatory security quality gates.	9.2	More Details
CVE-2026-26988	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below contain an SQL Injection vulnerability in the ajax_table.php endpoint. The application fails to properly sanitize or parameterize user input when processing IPv6 address searches. Specifically, the address parameter is split into an address and a prefix, and the prefix portion is directly concatenated into the SQL query string without validation. This allows an attacker to inject arbitrary SQL commands, potentially leading to unauthorized data access or database manipulation. This issue has been fixed in version 26.2.0.	9.1	More Details
CVE-2025-40538	A broken access control vulnerability exists in Serv-U which when exploited, gives a malicious actor the ability to create a system admin user and execute arbitrary code as a privileged account via domain admin or group admin privileges. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details
CVE-2025-13590	A malicious actor with administrative privileges can upload an arbitrary file to a user-controlled location within the deployment via a system REST API. Successful uploads may lead to remote code execution. By leveraging the vulnerability, a malicious actor may perform Remote Code Execution by uploading a specially crafted payload.	9.1	More Details
CVE-2025-40541	An Insecure Direct Object Reference (IDOR) vulnerability exists in Serv-U, which when exploited, gives a malicious actor the ability to execute native code as a privileged account. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details
CVE-2025-55853	SoftVision webPDF before 10.0.2 is vulnerable to Server-Side Request Forgery (SSRF). The PDF converter function does not check if internal or external resources are requested in the uploaded files and allows for protocols such as http:// and file:///. This allows an attacker to upload an XML or HTML file in the application, which when rendered to a PDF allows for internal port scanning and Local File Inclusion (LFI).	9.1	More Details
CVE-2025-40540	A type confusion vulnerability exists in Serv-U which when exploited, gives a malicious actor the ability to execute arbitrary native code as privileged account. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details
CVE-2025-40539	A type confusion vulnerability exists in Serv-U which when exploited, gives a malicious actor the ability to execute arbitrary native code as privileged account. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details
CVE-2026-27515	Binardat 10G08-0800GSM network switch firmware versions prior to V300SP10260209 generate predictable numeric session identifiers in the web management interface. An attacker can guess valid session IDs and hijack authenticated sessions.	9.1	More Details
CVE-2026-25548	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A critical Remote Code Execution (RCE) vulnerability exists in InvoicePlane 1.7.0 through a chained Local File Inclusion (LFI) and Log Poisoning attack. An authenticated administrator can execute arbitrary system commands on the server by manipulating the `public_invoice_template` setting to include poisoned log files containing PHP code. Version 1.7.1 patches the issue.	9.1	More Details
CVE-2025-70146	Missing authentication in multiple administrative action scripts under /admin/ in ProjectWorlds Online Time Table Generator 1.0 allows remote attackers to perform unauthorized administrative operations (e.g.,adding records, deleting records) via direct HTTP requests to affected endpoints without a valid session.	9.1	More Details
CVE-2024-58041	Smolder versions through 1.51 for Perl uses insecure rand() function for cryptographic functions. Smolder 1.51 and earlier for Perl uses the rand() function as the default source of entropy, which is not cryptographically secure, for cryptographic functions. Specifically Smolder::DB::Developer uses the Data::Random library which specifically states that it is "Useful mostly for test programs". Data::Random uses the rand() function.	9.1	More Details
CVE-2025-70043	An issue pertaining to CWE-295: Improper Certificate Validation was discovered in Ayms node-To master. The application disables TLS/SSL certificate validation by setting 'rejectUnauthorized': false in TLS socket options	9.1	More Details
	Crypt::NaCl::Sodium versions through 2.001 for Perl has an integer overflow flaw on 32-bit systems. Sodium.xs casts a		

CVE-2026-2588	STRLEN (size_t) to unsigned long long when passing a length pointer to libsodium functions. On 32-bit systems size_t is typically 32-bits while an unsigned long long is at least 64-bits.	9.1	More Details
CVE-2026-27471	ERP is a free and open source Enterprise Resource Planning tool. In versions up to 15.98.0 and 16.0.0-rc.1 and through 16.6.0, certain endpoints lacked access validation which allowed for unauthorized document access. This issue has been fixed in versions 15.98.1 and 16.6.1.	9.1	More Details
CVE-2026-27197	Sentry is a developer-first error tracking and performance monitoring tool. Versions 21.12.0 through 26.1.0 have a critical vulnerability in its SAML SSO implementation which allows an attacker to take over any user account by using a malicious SAML Identity Provider and another organization on the same Sentry instance. Self-hosted users are only at risk if the following criteria is met: ore than one organizations are configured (SENTRY_SINGLE_ORGANIZATION = True), or malicious user has existing access and permissions to modify SSO settings for another organization in a multo-organization instance. This issue has been fixed in version 26.2.0. To workaround this issue, implement user account-based two-factor authentication to prevent an attacker from being able to complete authentication with a victim's user account. Organization administrators cannot do this on a user's behalf, this requires individual users to ensure 2FA has been enabled for their account.	9.1	More Details
CVE-2026-26747	A Host Header Poisoning vulnerability exists in Monica 4.1.2 due to improper handling of the HTTP Host header in app/Providers/AppServiceProvider.php, combined with the default misconfiguration where the "app.force_url" is not set and default is "false". The application generates absolute URLs (such as those used in password reset emails) using the user-supplied Host header. This allows remote attackers to poison the password reset link sent to a victim,	9.1	More Details
CVE-2026-23552	Cross-Realm Token Acceptance Bypass in KeycloakSecurityPolicy Apache Camel Keycloak component. The Camel-Keycloak KeycloakSecurityPolicy does not validate the iss (issuer) claim of JWT tokens against the configured realm. A token issued by one Keycloak realm is silently accepted by a policy configured for a completely different realm, breaking tenant isolation. This issue affects Apache Camel: from 4.15.0 before 4.18.0. Users are recommended to upgrade to version 4.18.0, which fixes the issue.	9.1	More Details
CVE-2026-0573	An URL redirection vulnerability was identified in GitHub Enterprise Server that allowed attacker-controlled redirects to leak sensitive authorization tokens. The repository_pages API insecurely followed HTTP redirects when fetching artifact URLs, preserving the authorization header containing a privileged JWT. An authenticated user could redirect these requests to an attacker-controlled domain, exfiltrate the Actions.ManageOrgs JWT, and leverage it for potential remote code execution. Attackers would require access to the target GitHub Enterprise Server instance and the ability to exploit a legacy redirect to an attacker-controlled domain. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.19 and was fixed in versions 3.19.2, 3.18.4, 3.17.10, 3.16.13, 3.15.17, and 3.14.22. This vulnerability was reported via the GitHub Bug Bounty program.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-27169	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Versions 1.1.2-alpha and below render untrusted user/model content in chat tool UI surfaces using unsafe HTML interpolation patterns, leading to XSS. Stored content can execute JavaScript when later viewed in authenticated sessions. An attacker who can influence stored study/quiz/flashcard content could trigger script execution in a victim’s browser, potentially performing actions as that user in the local app session. This issue has been fixed in version 1.1.3-alpha.	8.9	More Details
CVE-2026-2904	A vulnerability was determined in UTT HiPER 810G 1.7.7-171114. This affects the function strcpy of the file /goform/ConfigExceptAli. Executing a manipulation can lead to buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2908	A security vulnerability has been detected in Tenda HG9 300001138. Affected by this issue is some unknown functionality of the file /boaform/formLoopBack of the component Loopback Detection Configuration Endpoint. Such manipulation of the argument Ethtype leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-69294	Deserialization of Untrusted Data vulnerability in fuelthemes PeakShops peakshops allows Object Injection.This issue affects PeakShops: from n/a through <= 1.5.9.	8.8	More Details
CVE-2026-2907	A weakness has been identified in Tenda HG9 300001138. Affected by this vulnerability is an unknown functionality of the file /boaform/formgponConf of the component GPON Configuration Endpoint. This manipulation of the argument fmgpon_loid/fmgpon_loid_password causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-2906	A security flaw has been discovered in Tenda HG9 300001138. Affected is an unknown function of the file /boaform/formSamba of the component Samba Configuration Endpoint. The manipulation of the argument sambaCap results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2025-70151	code-projects Scholars Tracking System 1.0 allows an authenticated attacker to achieve remote code execution via unrestricted file upload. The endpoints update_profile_picture.php and upload_picture.php store uploaded files in a web-accessible uploads/ directory using the original, user-supplied filename without validating the file type or extension. By uploading a PHP file and then requesting it from /uploads/, an attacker can execute arbitrary PHP code as the web server user.	8.8	More Details
CVE-2026-2905	A vulnerability was identified in Tenda HG9 300001138. This impacts an unknown function of the file /boaform/formWlanSetup of the component Wireless Configuration Endpoint. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-	A flaw has been found in D-Link DWR-M960 1.01.07. This impacts the function sub_4611CC of the file /boafrm/formNtp of the		

2026-2854	component NTP Configuration Endpoint. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-2909	A vulnerability was detected in Tenda HG9 300001138. This affects an unknown part of the file /boaform/formPing of the component Diagnostic Ping Endpoint. Performing a manipulation of the argument pingAddr results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-2886	A weakness has been identified in Tenda A21 1.0.0.0. This affects the function set_device_name of the file /goform/SetOnlineDevName. This manipulation of the argument devName causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-2885	A security flaw has been discovered in D-Link DWR-M960 1.01.07. The impacted element is the function sub_469104 of the file /boafrm/formIpv6Setup. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-2884	A vulnerability was identified in D-Link DWR-M960 1.01.07. The affected element is the function sub_41914C of the file /boafrm/formWanConfigSetup of the component WAN Interface Setting Handler. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-2883	A vulnerability was determined in D-Link DWR-M960 1.01.07. Impacted is the function sub_427D74 of the file /boafrm/formIpQoS. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2882	A vulnerability was found in D-Link DWR-M960 1.01.07. This issue affects the function sub_46385C of the file /boafrm/formDosCfg. Performing a manipulation of the argument submit-url results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-70064	PHPGurukul Hospital Management System v4.0 contains a Privilege Escalation vulnerability. A low-privileged user (Patient) can directly access the Administrator Dashboard and all sub-modules (e.g., User Logs, Doctor Management) by manually browsing to the /admin/ directory after authentication. This allows any self-registered user to takeover the application, view confidential logs, and modify system data.	8.8	More Details
CVE-2025-69328	Deserialization of Untrusted Data vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Object Injection.This issue affects Booking and Rental Manager: from n/a through <= 2.5.9.	8.8	More Details
CVE-2026-2910	A flaw has been found in Tenda HG9 300001138. This vulnerability affects unknown code of the file /boaform/formPing6. Executing a manipulation of the argument pingAddr can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	8.8	More Details
CVE-2026-2877	A vulnerability has been found in Tenda A18 15.13.07.13. This affects the function strcpy of the file /goform/WifiExtraSet of the component Httpd Service. The manipulation of the argument wpapsk_crypto5g leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-2959	A vulnerability was detected in D-Link DWR-M960 1.01.07. Affected by this vulnerability is the function sub_44E0F8 of the file /boafrm/formNewSchedule. Performing a manipulation of the argument url results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.	8.8	More Details
CVE-2026-2981	A vulnerability was found in UTT HiPER 810G up to 1.7.7-1711. The affected element is the function strcpy of the file /goform/formTaskEdit_ap. The manipulation of the argument txtMin2 results in buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-68526	Deserialization of Untrusted Data vulnerability in A WP Life Modal Popup Box modal-popup-box allows Object Injection.This issue affects Modal Popup Box: from n/a through <= 1.6.1.	8.8	More Details
CVE-2026-2962	A vulnerability was found in D-Link DWR-M960 1.01.07. This vulnerability affects the function sub_460F30 of the file /boafrm/formDateReboot of the component Scheduled Reboot Configuration Endpoint. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-1426	The Advanced AJAX Product Filters plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.1.9.6 via deserialization of untrusted input in the shortcode_check function within the Live Composer compatibility layer. This makes it possible for authenticated attackers, with Author-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. Note: This vulnerability requires the Live Composer plugin to also be installed and active.	8.8	More Details
CVE-2026-2961	A vulnerability has been found in D-Link DWR-M960 1.01.07. This affects the function sub_4196C4 of the file /boafrm/formVpnConfigSetup of the component VPN Configuration Endpoint. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-2960	A flaw has been found in D-Link DWR-M960 1.01.07. Affected by this issue is the function sub_468D64 of the file /boafrm/formDhcpv6s. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-2958	A security vulnerability has been detected in D-Link DWR-M960 1.01.07. Affected is the function sub_457C5C of the file /boafrm/formWsc. Such manipulation of the argument save_apply leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details

CVE-2026-2911	A vulnerability has been found in Tenda FH451 up to 1.0.0.9. This issue affects some unknown processing of the file /goform/GstDhcpSetSer. The manipulation leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-68531	Deserialization of Untrusted Data vulnerability in modeltheme ModelTheme Addons for WPBakery and Elementor modeltheme-addons-for-wpbakery allows Object Injection.This issue affects ModelTheme Addons for WPBakery and Elementor: from n/a through < 1.5.6.	8.8	More Details
CVE-2026-2929	A vulnerability was determined in D-Link DWR-M960 1.01.07. Impacted is the function sub_453140 of the file /boafrm/formWlAc of the component Wireless Access Control Endpoint. This manipulation of the argument submit-url causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2928	A vulnerability was found in D-Link DWR-M960 1.01.07. This issue affects the function sub_452CCC of the file /boafrm/formWlEncrypt of the component WLAN Encryption Configuration Endpoint. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-2926	A flaw has been found in D-Link DWR-M960 1.01.07. This affects the function sub_4237AC of the file /boafrm/formLteSetup of the component LTE Configuration Endpoint. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-2925	A vulnerability was detected in D-Link DWR-M960 1.01.07. Affected by this issue is the function sub_42B5A0 of the file /boafrm/formBridgeVlan of the component Bridge VLAN Configuration Endpoint. Performing a manipulation of the argument submit-url results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-68853	Deserialization of Untrusted Data vulnerability in Kleor Contact Manager contact-manager allows Object Injection.This issue affects Contact Manager: from n/a through <= 9.1.1.	8.8	More Details
CVE-2026-2881	A vulnerability has been found in D-Link DWR-M960 1.01.07. This vulnerability affects the function sub_425FF8 of the file /boafrm/formFirewallAdv of the component Advanced Firewall Configuration Endpoint. Such manipulation of the argument submit-url leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-2876	A vulnerability was determined in Tenda A18 15.13.07.13. This affects the function parse_macfilter_rule of the file /goform/setBlackRule. This manipulation of the argument deviceList causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-3016	A vulnerability was identified in UTT HiPER 810G up to 1.7.7-171114. The affected element is the function strcpy of the file /goform/formP2PLimitConfig. The manipulation of the argument except leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-2853	A vulnerability was detected in D-Link DWR-M960 1.01.07. This affects the function sub_462E14 of the file /boafrm/formSysLog of the component System Log Configuration Endpoint. Performing a manipulation of the argument submit-url results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-2041	Nagios Host zabbixagent_configwizard_func Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Nagios Host. Authentication is required to exploit this vulnerability. The specific flaw exists within the zabbixagent_configwizard_func method. 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 execute code in the context of the service account. Was ZDI-CAN-28250.	8.8	More Details
CVE-2026-25232	Gogs is an open source self-hosted Git service. Versions 0.13.4 and below have an access control bypass vulnerability which allows any repository collaborator with Write permissions to delete protected branches (including the default branch) by sending a direct POST request, completely bypassing the branch protection mechanism. This vulnerability in the DeleteBranchPost function eenables privilege escalation from Write to Admin level, allowing low-privilege users to perform dangerous operations that should be restricted to administrators only. Although Git Hook layer correctly prevents protected branch deletion via SSH push, the web interface deletion operation does not trigger Git Hooks, resulting in complete bypass of protection mechanisms. In oder to exploit this vulnerability, attackers must have write permissions to the target repository, protected branches configured to the target repository and access to the Gogs web interface. This issue has been fixed in version 0.14.1.	8.8	More Details
CVE-2018-25158	Chamilo LMS 1.11.8 contains an arbitrary file upload vulnerability that allows authenticated users to upload and execute PHP files through the elfinder filemanager module. Attackers can upload files with image headers in the social myfiles section, rename them to PHP extensions, and execute arbitrary code by accessing the uploaded files.	8.8	More Details
CVE-2026-2857	A vulnerability was determined in D-Link DWR-M960 1.01.07. Affected by this issue is the function sub_423E00 of the file /boafrm/formPortFw of the component Port Forwarding Configuration Endpoint. This manipulation of the argument submit-url causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2856	A vulnerability was found in D-Link DWR-M960 1.01.07. Affected by this vulnerability is the function sub_424AFC of the file /boafrm/formFilter of the component Filter Configuration Endpoint. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-2855	A vulnerability has been found in D-Link DWR-M960 1.01.07. Affected is the function sub_4648F0 of the file /boafrm/formDdns of the component DDNS Settings Handler. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-	The NewsBlogger theme for WordPress is vulnerable to Cross-Site Request Forgery in versions 0.2.5.6 to 0.2.6.1. This is due to missing or incorrect nonce validation on the newsblogger_install_and_activate_plugin() function. This makes it possible for		More

12821	unauthenticated attackers to upload arbitrary files and achieve remote code execution via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This is due to a reverted fix of CVE-2025-1305.	8.8	Details
CVE-2026-2874	A flaw has been found in Tenda A21 1.0.0.0. Impacted is the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. Executing a manipulation of the argument ssid can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-12845	The Tablesome Table – Contact Form DB – WPForms, CF7, Gravity, Forminator, Fluent plugin for WordPress is vulnerable to unauthorized access of data that leads to privilege escalation due to a missing capability check on the get_table_data() function in versions 0.5.4 to 1.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve plugin table data that can expose email log information. Attackers can leverage this on sites where the table log is enabled in order to trigger a password reset and obtain the reset key.	8.8	More Details
CVE-2026-0974	The Orderable – WordPress Restaurant Online Ordering System and Food Ordering Plugin plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the 'install_plugin' function in all versions up to, and including, 1.20.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install arbitrary plugins, which can lead to Remote Code Execution.	8.8	More Details
CVE-2026-0912	The Toret Manager plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'trman_save_option' function and on the 'trman_save_option_items' in all versions up to, and including, 1.2.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	8.8	More Details
CVE-2026-26746	OpenSourcePOS 3.4.1 contains a Local File Inclusion (LFI) vulnerability in the Sales.php::getInvoice() function. An attacker can read arbitrary files on the web server by manipulating the Invoice Type configuration. This issue can be chained with the file upload functionality to achieve Remote Code Execution (RCE).	8.8	More Details
CVE-2025-13603	The WP AUDIO GALLERY plugin for WordPress is vulnerable to Unauthorized Arbitrary File Read in all versions up to, and including, 2.0. This is due to insufficient capability checks and lack of nonce verification on the "wpag_htaccess_callback" function This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the site's .htaccess file with arbitrary content, which can lead to arbitrary file read on the server under certain configurations.	8.8	More Details
CVE-2025-4521	The IDonate – Blood Donation, Request And Donor Management System plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the idonate_donor_profile() function in versions 2.1.5 to 2.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to hijack any account by reassigning its email address (via the donor_id they supply) and then triggering a password reset, ultimately granting themselves full administrator privileges.	8.8	More Details
CVE-2026-2042	Nagios Host monitoringwizard Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Nagios Host. Authentication is required to exploit this vulnerability. The specific flaw exists within the monitoringwizard module. 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 execute code in the context of the service account. Was ZDI-CAN-28245.	8.8	More Details
CVE-2026-2043	Nagios Host esensors_websensor_configwizard_func Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Nagios Host. Authentication is required to exploit this vulnerability. The specific flaw exists within the esensors_websensor_configwizard_func method. 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 execute code in the context of the service account. Was ZDI-CAN-28249.	8.8	More Details
CVE-2026-27168	SAIL is a cross-platform library for loading and saving images with support for animation, metadata, and ICC profiles. All versions are vulnerable to Heap-based Buffer Overflow through the XWD parser's use of the bytes_per_line value. The value os read directly from the file as the read size in io->strict_read(), and is never compared to the actual size of the destination buffer. An attacker can provide an XWD file with an arbitrarily large bytes_per_line, causing a massive write operation beyond the buffer heap allocated for the image pixels. The issue did not have a fix at the time of publication.	8.8	More Details
CVE-2026-2650	Heap buffer overflow in Media in Google Chrome prior to 145.0.7632.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-2649	Integer overflow in V8 in Google Chrome prior to 145.0.7632.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-2648	Heap buffer overflow in PDFium in Google Chrome prior to 145.0.7632.109 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-22354	Deserialization of Untrusted Data vulnerability in Dotstore Woocommerce Category Banner Management banner-management-for-woocommerce allows Object Injection.This issue affects Woocommerce Category Banner Management: from n/a through <= 2.5.1.	8.8	More Details
CVE-2026-22346	Deserialization of Untrusted Data vulnerability in A WP Life Slider Responsive Slideshow – Image slider, Gallery slideshow slider-responsive-slideshow allows Object Injection.This issue affects Slider Responsive Slideshow – Image slider, Gallery slideshow: from n/a through <= 1.5.4.	8.8	More Details
CVE-2026-22345	Deserialization of Untrusted Data vulnerability in A WP Life Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery new-image-gallery allows Object Injection.This issue affects Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery: from n/a through <= 1.6.0.	8.8	More Details
	Formwork is a flat file-based Content Management System (CMS). In versions 2.0.0 through 2.3.3, the application fails to		

CVE-2026-27198	properly enforce role-based authorization during account creation. Although the system validates that the specified role exists, it does not verify whether the current user has sufficient privileges to assign highly privileged roles such as admin. As a result, an authenticated user with the editor role can create a new account with administrative privileges, leading to full administrative access and complete compromise of the CMS. This issue has been fixed in version 2.3.4.	8.8	More Details
CVE-2019-25351	Centova Cast 3.2.11 contains a file download vulnerability that allows authenticated attackers to retrieve arbitrary system files through the server.copyfile API endpoint. Attackers can exploit the vulnerability by supplying crafted parameters to download sensitive files like /etc/passwd using curl and wget requests.	8.8	More Details
CVE-2026-23544	Deserialization of Untrusted Data vulnerability in codetipi Valenti valenti allows Object Injection.This issue affects Valenti: from n/a through <= 5.6.3.5.	8.8	More Details
CVE-2026-27470	ZoneMinder is a free, open source closed-circuit television software application. In versions 1.36.37 and below and 1.37.61 through 1.38.0, there is a second-order SQL Injection vulnerability in the web/ajax/status.php file within the getNearEvents() function. Event field values (specifically Name and Cause) are stored safely via parameterized queries but are later retrieved and concatenated directly into SQL WHERE clauses without escaping. An authenticated user with Events edit and view permissions can exploit this to execute arbitrary SQL queries.	8.8	More Details
CVE-2026-2870	A security flaw has been discovered in Tenda A21 1.0.0.0. Affected by this issue is the function set_qosMib_list of the file /goform/formSetQosBand. The manipulation of the argument list results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-2871	A weakness has been identified in Tenda A21 1.0.0.0. This affects the function fromSetIpMacBind of the file /goform/SetIpMacBind. This manipulation of the argument list causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-2872	A security vulnerability has been detected in Tenda A21 1.0.0.0. This vulnerability affects the function set_device_name of the file /goform/setBlackRule of the component MAC Filtering Configuration Endpoint. Such manipulation of the argument devName/mac leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-2873	A vulnerability was detected in Tenda A21 1.0.0.0. This issue affects the function setSchedWifi of the file /goform/openSchedWifi. Performing a manipulation of the argument schedStartTime/schedEndTime results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-3015	A vulnerability was determined in UTT HiPER 810G up to 1.7.7-171114. Impacted is the function strcpy of the file /goform/formPolicyRouteConf. Executing a manipulation of the argument GroupName can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2927	A vulnerability has been found in D-Link DWR-M960 1.01.07. This vulnerability affects the function sub_462590 of the file /boafrm/formOpMode of the component Operation Mode Configuration Endpoint. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-26331	yt-dlp is a command-line audio/video downloader. Starting in version 2023.06.21 and prior to version 2026.02.21, when yt-dlp's `--netrc-cmd` command-line option (or `netrc_cmd` Python API parameter) is used, an attacker could achieve arbitrary command injection on the user's system with a maliciously crafted URL. yt-dlp maintainers assume the impact of this vulnerability to be high for anyone who uses `--netrc-cmd` in their command/configuration or `netrc_cmd` in their Python scripts. Even though the maliciously crafted URL itself will look very suspicious to many users, it would be trivial for a maliciously crafted webpage with an inconspicuous URL to covertly exploit this vulnerability via HTTP redirect. Users without `--netrc-cmd` in their arguments or `netrc_cmd` in their scripts are unaffected. No evidence has been found of this exploit being used in the wild. yt-dlp version 2026.02.21 fixes this issue by validating all netrc "machine" values and raising an error upon unexpected input. As a workaround, users who are unable to upgrade should avoid using the `--netrc-cmd` command-line option (or `netrc_cmd` Python API parameter), or they should at least not pass a placeholder (`{}`) in their `--netrc-cmd` argument.	8.8	More Details
CVE-2026-26358	Dell Unisphere for PowerMax, version(s) 10.2, contain(s) a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	8.8	More Details
CVE-2026-26990	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below have a Time-Based Blind SQL Injection vulnerability in address-search.inc.php via the address parameter. When a crafted subnet prefix is supplied, the prefix value is concatenated directly into an SQL query without proper parameter binding, allowing an attacker to manipulate query logic and infer database information through time-based conditional responses. This vulnerability requires authentication and is exploitable by any authenticated user. This issue has been fixedd in version 26.2.0.	8.8	More Details
CVE-2026-26065	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Versions 9.2.1 and below are vulnerable to Path Traversal through PDB readers (both 132-byte and 202-byte header variants) that allow arbitrary file writes with arbitrary extension and arbitrary content anywhere the user has write permissions. Files are written in 'wb' mode, silently overwriting existing files. This can lead to potential code execution and Denial of Service through file corruption. This issue has been fixed in version 9.3.0.	8.8	More Details
CVE-2026-26064	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Versions 9.2.1 and below contain a Path Traversal vulnerability that allows arbitrary file writes anywhere the user has write permissions. On Windows, this leads to Remote Code Execution by writing a payload to the Startup folder, which executes on next login. Function extract_pictures only checks startswith('Pictures'), and does not sanitize '..' sequences. calibre's own ZipFile.extractall() in utils/zipfile.py does sanitize '..' via _get_targetpath(), but extract_pictures() bypasses this by using manual zf.read() + open(). This issue has been fixed in version 9.3.0.	8.8	More Details
	Music Assistant is an open-source media library manager that integrates streaming services with connected speakers. Versions 2.6.3 and below allow unauthenticated network-adjacent attackers to execute arbitrary code on affected installations. The		

CVE-2026-26975	music/playlists/update API allows users to bypass the .m3u extension enforcement and write files anywhere on the filesystem, which is exacerbated by the container running as root. This can be exploited to achieve Remote Code Execution by writing a malicious .pth file to the Python site-packages directory, which will execute arbitrary commands when Python loads. This issue has been fixed in version 2.7.0.	8.8	More Details
CVE-2026-3044	A vulnerability has been found in Tenda AC8 16.03.34.06. This affects the function webCgiGetUploadFile of the file /cgi-bin/UploadCfg of the component Httpd Service. The manipulation of the argument boundary leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-15560	An authenticated attacker with minimal permissions can exploit a SQL injection in the WorkTime server "widget" API endpoint to inject SQL queries. If the Firebird backend is used, attackers are able to retrieve all data from the database backend. If the MSSQL backend is used the attacker can execute arbitrary SQL statements on the database backend and gain access to sensitive data.	8.8	More Details
CVE-2026-26323	OpenClaw is a personal AI assistant. Versions 2026.1.8 through 2026.2.13 have a command injection in the maintainer/dev script `scripts/update-clawtributors.ts`. The issue affects contributors/maintainers (or CI) who run `bun scripts/update-clawtributors.ts` in a source checkout that contains a malicious commit author email (e.g. crafted `@users[.]noreply[.]github[.]com` values). Normal CLI usage is not affected (`npm i -g openclaw`): this script is not part of the shipped CLI and is not executed during routine operation. The script derived a GitHub login from `git log` author metadata and interpolated it into a shell command (via `execSync`). A malicious commit record could inject shell metacharacters and execute arbitrary commands when the script is run. Version 2026.2.14 contains a patch.	8.8	More Details
CVE-2025-13943	A post-authentication command injection vulnerability in the log file download function of the Zyxel EX3301-T0 firmware versions through 5.50(ABVY.7)C0 could allow an authenticated attacker to execute operating system (OS) commands on an affected device.	8.8	More Details
CVE-2026-26318	systeminformation is a System and OS information library for node.js. Versions prior to 5.31.0 are vulnerable to command injection via unsanitized `locate` output in `versions()`. Version 5.31.0 fixes the issue.	8.8	More Details
CVE-2025-15386	The Responsive Lightbox & Gallery WordPress plugin before 2.6.1 is vulnerable to an Unauthenticated Stored-XSS attack due to flawed regex replacement rules that can be abused by posting a comment with a malicious link when lightbox for comments are enabled and then approved.	8.8	More Details
CVE-2026-2769	Use-after-free in the Storage: IndexedDB component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	8.8	More Details
CVE-2026-2798	Use-after-free in the DOM: Core & HTML component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	8.8	More Details
CVE-2026-27483	MindsDB is a platform for building artificial intelligence from enterprise data. Prior to version 25.9.1.1, there is a path traversal vulnerability in Mindsdb's /api/files interface, which an authenticated attacker can exploit to achieve remote command execution. The vulnerability exists in the "Upload File" module, which corresponds to the API endpoint /api/files. Since the multipart file upload does not perform security checks on the uploaded file path, an attacker can perform path traversal by using `../` sequences in the filename field. The file write operation occurs before calling clear_filename and save_file, meaning there is no filtering of filenames or file types, allowing arbitrary content to be written to any path on the server. Version 25.9.1.1 patches the issue.	8.8	More Details
CVE-2026-23678	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior contain a command injection vulnerability in the traceroute diagnostic function of the affected device web management interface. By injecting the %1a character into the hostname parameter, an authenticated attacker with access to the web interface can execute arbitrary CLI commands on the device.	8.8	More Details
CVE-2026-22765	Dell Wyse Management Suite, versions prior to WMS 5.5, contain a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of Privileges.	8.8	More Details
CVE-2026-26359	Dell Unisphere for PowerMax, version(s) 10.2, contain(s) an External Control of File Name or Path vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to the ability to overwrite arbitrary files.	8.8	More Details
CVE-2026-22384	Deserialization of Untrusted Data vulnerability in leafcolor Applay - Shortcodes applay-shortcodes allows Object Injection.This issue affects Applay - Shortcodes: from n/a through <= 3.7.	8.8	More Details
CVE-2026-25648	Versions of the Traccar open-source GPS tracking system starting with 6.11.1 contain an issue in which authenticated users can execute arbitrary JavaScript in the context of other users' browsers by uploading malicious SVG files as device images. The application accepts SVG file uploads without sanitization and serves them with the `image/svg+xml` Content-Type, allowing embedded JavaScript to execute when victims view the image. As of time of publication, it is unclear whether a fix is available.	8.7	More Details
CVE-2026-1714	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution plugin for WordPress is vulnerable to Email Relay Abuse in all versions up to, and including, 3.3.2. This is due to the lack of validation on the 'send_to', 'product_title', 'wlmessage', and 'wlemail' parameters in the 'woolentor_suggest_price_action' AJAX endpoint. This makes it possible for unauthenticated attackers to send arbitrary emails to any recipient with full control over the subject line, message content, and sender address (via CRLF injection in the 'wlemail' parameter), effectively turning the website into a full email relay for spam or phishing campaigns.	8.6	More Details
	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, ImageMagick's path security policy is enforced on the raw filename string before the filesystem resolves it. As a		

CVE-2026-25965	result, a policy rule such as /etc/* can be bypassed by a path traversal. The OS resolves the traversal and opens the sensitive file, but the policy matcher only sees the unnormalized path and therefore allows the read. This enables local file disclosure (LFI) even when policy-secure.xml is applied. Actions to prevent reading from files have been taken in versions .7.1.2-15 and 6.9.13-40 But it make sure writing is also not possible the following should be added to one's policy. This will also be included in ImageMagick's more secure policies by default.	8.6	More Details
CVE-2025-69063	Missing Authorization vulnerability in Saad Iqbal New User Approve new-user-approve allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects New User Approve: from n/a through <= 3.2.0.	8.6	More Details
CVE-2026-24959	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JoomSky JS Help Desk js-support-ticket allows Blind SQL Injection.This issue affects JS Help Desk: from n/a through <= 3.0.1.	8.5	More Details
CVE-2025-67733	Valkey is a distributed key-value database. Prior to versions 9.0.2, 8.1.6, 8.0.7, and 7.2.12, a malicious user can use scripting commands to inject arbitrary information into the response stream for the given client, potentially corrupting or returning tampered data to other users on the same connection. The error handling code for lua scripts does not properly handle null characters. Versions 9.0.2, 8.1.6, 8.0.7, and 7.2.12 fix the issue.	8.5	More Details
CVE-2026-26286	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. In versions prior to 1.16.0, a Server-Side Request Forgery (SSRF) vulnerability in the asset download endpoint allows authenticated users to make arbitrary HTTP requests from the server and read the full response body, enabling access to internal services, cloud metadata, and private network resources. The vulnerability has been patched in the version 1.16.0 by introducing a whitelist domain check for asset download requests. It can be reviewed and customized by editing the `whitelistImportDomains` array in the `config.yaml` file.	8.5	More Details
CVE-2025-67987	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ExpressTech Systems Quiz And Survey Master quiz-master-next allows SQL Injection.This issue affects Quiz And Survey Master: from n/a through <= 10.3.1.	8.5	More Details
CVE-2024-56373	DAG Author (who already has quite a lot of permissions) could manipulate database of Airflow 2 in the way to execute arbitrary code in the web-server context, which they should normally not be able to do, leading to potentially remote code execution in the context of web-server (server-side) as a result of a user viewing historical task information. The functionality responsible for that (log template history) has been disabled by default in 2.11.1 and users should upgrade to Airflow 3 if they want to continue to use log template history. They can also manually modify historical log file names if they want to see historical logs that were generated before the last log template change.	8.4	More Details
CVE-2026-26280	systeminformation is a System and OS information library for node.js. In versions prior to 5.30.8, a command injection vulnerability in the `wifiNetworks()` function allows an attacker to execute arbitrary OS commands via an unsanitized network interface parameter in the retry code path. In `lib/wifi.js`, the `wifiNetworks()` function sanitizes the `iface` parameter on the initial call (line 437). However, when the initial scan returns empty results, a `setTimeout` retry (lines 440-441) calls `getWifiNetworkListIw(iface)` with the **original unsanitized** `iface` value, which is passed directly to `execSync('iwlist ${iface} scan')`. Any application passing user-controlled input to `si.wifiNetworks()` is vulnerable to arbitrary command execution with the privileges of the Node.js process. Version 5.30.8 fixes the issue.	8.4	More Details
CVE-2019-25357	Control Center PRO 6.2.9 contains a stack-based buffer overflow vulnerability in the user creation module's username field that allows attackers to overwrite Structured Exception Handler (SEH). Attackers can craft a malicious payload exceeding 664 bytes to inject shellcode and potentially execute arbitrary code on vulnerable Windows systems.	8.4	More Details
CVE-2026-27182	Saturn Remote Mouse Server contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary commands by sending specially crafted UDP JSON frames to port 27000. Attackers on the local network can send malformed packets with unsanitized command data that the service forwards directly to OS execution functions, enabling remote code execution under the service account.	8.4	More Details
CVE-2026-27203	eBay API MCP Server is an open source local MCP server providing AI assistants with comprehensive access to eBay's Sell APIs. All versions are vulnerable to Environment Variable Injection through the updateEnvFile function. The ebay_set_user_tokens tool allows updating the .env file with new tokens. The updateEnvFile function in src/auth/oauth.ts blindly appends or replaces values without validating them for newlines or quotes. This allows an attacker to inject arbitrary environment variables into the configuration file. An attacker can inject arbitrary environment variables into the .env file. This could lead to configuration overwrites, Denial of Service, and potential RCE. There was no fix for this issue at the time of publication.	8.3	More Details
CVE-2026-1367	Zohocorp ManageEngine ADSelfService Plus versions 6522 and below are vulnerable to authenticated SQL Injection in the search report option.	8.3	More Details
CVE-2026-26337	Hyland Alfresco Transformation Service allows unauthenticated attackers to achieve both arbitrary file read and server-side request forgery through the absolute path traversal.	8.2	More Details
CVE-2025-67977	Missing Authorization vulnerability in VillaTheme HAPPY happy-helpdesk-support-ticket-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HAPPY: from n/a through <= 1.0.8.	8.2	More Details
CVE-2019-25446	DIGIT CENTRIS ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the datum1, datum2, KID, and PID parameters. Attackers can send POST requests to /korisnikinfo.php with malicious SQL syntax in these parameters to extract or modify sensitive database information.	8.2	More Details
CVE-2019-25443	Inventory Webapp contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters. Attackers can supply malicious SQL payloads in the name, description, quantity, or cat_id parameters to add-item.php to execute arbitrary database commands.	8.2	More Details
CVE-	ImageMagick is free and open-source software used for editing and manipulating digital images. `WriteUHDRImage` in		

2026-25794	`coders/uhdr.c` uses `int` arithmetic to compute the pixel buffer size. Prior to version 7.1.2-15, when image dimensions are large, the multiplication overflows 32-bit `int`, causing an undersized heap allocation followed by an out-of-bounds write. This can crash the process or potentially lead to an out of bounds heap write. Version 7.1.2-15 contains a patch.	8.2	More Details
CVE-2019-25442	Web Wiz Forums 12.01 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the PF parameter. Attackers can send GET requests to member_profile.asp with malicious PF values to extract sensitive database information.	8.2	More Details
CVE-2019-25440	WebIncorp ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the prod_id parameter. Attackers can send GET requests to product_detail.php with malicious prod_id values to extract sensitive database information.	8.2	More Details
CVE-2026-2818	A zip-slip path traversal vulnerability in Spring Data Geode's import snapshot functionality allows attackers to write files outside the intended extraction directory. This vulnerability appears to be susceptible on Windows OS only.	8.2	More Details
CVE-2019-25433	XOOPS CMS 2.5.9 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cid parameter. Attackers can send GET requests to the gerar_pdf.php endpoint with malicious cid values to extract sensitive database information.	8.2	More Details
CVE-2019-25366	microASP Portal+ CMS contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the explode_tree parameter. Attackers can send crafted requests to pagina.phtml with SQL injection payloads using extractvalue and concat functions to extract sensitive database information like the current database name.	8.2	More Details
CVE-2026-27179	MajorDoMo (aka Major Domestic Module) contains an unauthenticated SQL injection vulnerability in the commands module. The commands_search.inc.php file directly interpolates the $_GET['parent'] parameter into multiple SQL queries without sanitization or parameterized queries. The commands module is loadable without authentication via the /objects/?module=commands endpoint, which includes arbitrary modules by name and calls their usual() method. Time-based blind SQL injection is exploitable using UNION SELECT SLEEP() syntax. Because MajorDoMo stores admin passwords as unsalted MD5 hashes in the users table, successful exploitation enables extraction of credentials and subsequent admin panel access.	8.2	More Details
CVE-2019-25444	Fiverr Clone Script 1.2.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the page parameter. Attackers can supply malicious SQL syntax in the page parameter to extract sensitive database information or modify database contents.	8.2	More Details
CVE-2019-25452	Dolibarr ERP/CRM 10.0.1 contains an SQL injection vulnerability in the elemid POST parameter of the viewcat.php endpoint that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can submit crafted POST requests with malicious SQL payloads in the elemid parameter to extract sensitive database information using error-based or time-based blind SQL injection techniques.	8.2	More Details
CVE-2026-26723	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v. 20230721a allows a remote attacker to execute arbitrary code via the function parameter.	8.2	More Details
CVE-2019-25391	Ashop Shopping Cart Software contains a time-based blind SQL injection vulnerability that allows attackers to manipulate database queries through the blacklistitemid parameter. Attackers can send POST requests to the admin/bannedcustomers.php endpoint with crafted SQL payloads using SLEEP functions to extract sensitive database information.	8.2	More Details
CVE-2019-25439	NoviSmart CMS contains an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through the Referer HTTP header field. Attackers can craft requests with time-based SQL injection payloads in the Referer header to extract sensitive database information or cause denial of service.	8.2	More Details
CVE-2019-25455	Web Ofisi E-Ticaret v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'a' parameter. Attackers can send GET requests to with malicious 'a' parameter values to extract sensitive database information.	8.2	More Details
CVE-2026-24790	The underlying PLC of the device can be remotely influenced, without proper safeguards or authentication.	8.2	More Details
CVE-2026-21535	Improper access control in Microsoft Teams allows an unauthorized attacker to disclose information over a network.	8.2	More Details
CVE-2019-25431	delpino73 Blue-Smiley-Organizer 1.32 contains an SQL injection vulnerability in the datetime parameter that allows unauthenticated attackers to manipulate database queries. Attackers can inject SQL code through POST requests to extract sensitive data using boolean-based blind and time-based blind techniques, or write files to the server using INTO OUTFILE statements.	8.2	More Details
CVE-2026-24708	An issue was discovered in OpenStack Nova before 30.2.2, 31 before 31.2.1, and 32 before 32.1.1. By writing a malicious QCOW header to a root or ephemeral disk and then triggering a resize, a user may convince Nova's Flat image backend to call qemu-img without a format restriction, resulting in an unsafe image resize operation that could destroy data on the host system. Only compute nodes using the Flat image backend (usually configured with use_cow_images=False) are affected.	8.2	More Details
CVE-2019-25359	SD.NET RIM versions before 4.7.3c contain a SQL injection vulnerability that allows attackers to inject malicious SQL statements through POST parameters 'idtyp' and 'idgremium'. Attackers can exploit this vulnerability by crafting specially formed POST requests to the /vorlagen/ endpoint, enabling unauthorized database manipulation and potential information disclosure.	8.2	More Details
CVE-2019-25438	LabCollector 5.423 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commands by injecting malicious code through POST parameters. Attackers can submit crafted SQL payloads in the login parameter of login.php or the user_name parameter of retrieve_password.php to extract sensitive database information without authentication.	8.2	More Details

CVE-2019-25456	Web Ofisi Emlak v2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'ara' GET parameter. Attackers can send requests to with time-based SQL injection payloads to extract sensitive database information or cause denial of service.	8.2	More Details
CVE-2019-25462	Web Ofisi Rent a Car v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'klima' parameter. Attackers can send GET requests to with malicious 'klima' values to extract sensitive database information or cause denial of service.	8.2	More Details
CVE-2019-25461	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' parameter. Attackers can send POST requests to the ajax/productsFilterSearch endpoint with malicious 'q' values using time-based blind SQL injection techniques to extract sensitive database information.	8.2	More Details
CVE-2019-25460	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' GET parameter. Attackers can send requests to the arama endpoint with malicious 'q' values using time-based SQL injection techniques to extract sensitive database information.	8.2	More Details
CVE-2019-25459	Web Ofisi Emlak V2 contains multiple SQL injection vulnerabilities in the endpoint that allow unauthenticated attackers to manipulate database queries through GET parameters. Attackers can inject SQL code into parameters like emlak_durumu, emlak_tipi, il, ilce, kelime, and semt to extract sensitive database information or perform time-based blind SQL injection attacks.	8.2	More Details
CVE-2019-25458	Web Ofisi Firma Rehberi v1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters. Attackers can send requests to with malicious payloads in the 'il', 'kat', or 'kelime' parameters to extract sensitive database information or perform time-based blind SQL injection attacks.	8.2	More Details
CVE-2019-25457	Web Ofisi Firma v13 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'oz' array parameter. Attackers can send GET requests to category pages with malicious 'oz[]' values using time-based blind SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2026-27475	SPIP before 4.4.9 allows Insecure Deserialization in the public area through the table_valeur filter and the DATA iterator, which accept serialized data. An attacker who can place malicious serialized content (a pre-condition requiring prior access or another vulnerability) can trigger arbitrary object instantiation and potentially achieve code execution. The use of serialized data in these components has been deprecated and will be removed in SPIP 5. This vulnerability is not mitigated by the SPIP security screen.	8.1	More Details
CVE-2026-27516	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior expose user passwords in plaintext within the administrative interface and HTTP responses, allowing recovery of valid credentials.	8.1	More Details
CVE-2026-22361	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes A-Mart a-mart allows PHP Local File Inclusion.This issue affects A-Mart: from n/a through <= 1.0.2.	8.1	More Details
CVE-2026-22364	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes SevenTrees seventrees allows PHP Local File Inclusion.This issue affects SevenTrees: from n/a through <=1.0.2.	8.1	More Details
CVE-2026-22363	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Rhodos rhodos allows PHP Local File Inclusion.This issue affects Rhodos: from n/a through <= 1.3.3.	8.1	More Details
CVE-2026-22362	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Photolia photolia allows PHP Local File Inclusion.This issue affects Photolia: from n/a through <= 1.0.3.	8.1	More Details
CVE-2025-69375	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SolverWp Portfolio Builder swp-portfolio allows PHP Local File Inclusion.This issue affects Portfolio Builder: from n/a through <= 1.2.5.	8.1	More Details
CVE-2026-22366	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Jude jude allows PHP Local File Inclusion.This issue affects Jude: from n/a through <= 1.3.0.	8.1	More Details
CVE-2026-27134	Strimzi provides a way to run an Apache Kafka cluster on Kubernetes or OpenShift in various deployment configurations. In versions 0.49.0 through 0.50.0, when using a custom Cluster or Clients CA with a multistage CA chain consisting of multiple CAs, Strimzi incorrectly configures the trusted certificates for mTLS authentication on the internal as well as user-configured listeners. All CAs from the CA chain will be trusted. And users with certificates signed by any of the CAs in the chain will be able to authenticate. This issue affects only users using a custom Cluster or Clients CA with a multistage CA chain consisting of multiple CAs. It does not affect users using the Strimzi-managed Cluster and Clients CAs. It also does not affect users using custom Cluster or Clients CA with only a single CA (i.e., no CA chain with multiple CAs). This issue has been fixed in version 0.50.1. To workaround this issue, instead of providing the full CA chain as the custom CA, users can provide only the single CA that should be used.	8.1	More Details
CVE-2025-60087	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Nenad Obradovic Extensive VC Addons for WPBakery page builder extensive-vc-addon allows PHP Local File Inclusion.This issue affects Extensive VC Addons for WPBakery page builder: from n/a through <= 1.9.1.	8.1	More Details
CVE-2025-67980	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Hara hara allows PHP Local File Inclusion.This issue affects Hara: from n/a through <= 1.2.17.	8.1	More Details

CVE-2025-69402	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX R&F rf allows PHP Local File Inclusion.This issue affects R&F: from n/a through <= 1.5.	8.1	More Details
CVE-2026-27196	Statmatic is a Laravel and Git powered content management system (CMS). Versions 5.73.8 and below in addition to 6.0.0-alpha.1 through 6.3.1 have a Stored XSS vulnerability in html fieldtypes which allows authenticated users with field management permissions to inject malicious JavaScript that executes when viewed by higher-privileged users. This issue has been fixed in 6.3.2 and 5.73.9.	8.1	More Details
CVE-2025-69410	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Belletrist belletrist allows PHP Local File Inclusion.This issue affects Belletrist: from n/a through <= 1.2.	8.1	More Details
CVE-2025-69409	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes PJ | Life & Business Coaching pj allows PHP Local File Inclusion.This issue affects PJ | Life & Business Coaching: from n/a through <= 3.0.0.	8.1	More Details
CVE-2025-69408	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes HealthFirst healthfirst allows PHP Local File Inclusion.This issue affects HealthFirst: from n/a through <= 1.0.1.	8.1	More Details
CVE-2025-69407	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Struktur struktur allows PHP Local File Inclusion.This issue affects Struktur: from n/a through <= 2.5.1.	8.1	More Details
CVE-2025-69406	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX FreightCo freightco allows PHP Local File Inclusion.This issue affects FreightCo: from n/a through <= 1.1.7.	8.1	More Details
CVE-2025-69400	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Yokoo yokoo allows PHP Local File Inclusion.This issue affects Yokoo: from n/a through <= 1.1.11.	8.1	More Details
CVE-2025-69395	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Gable gable allows PHP Local File Inclusion.This issue affects Gable: from n/a through <= 1.5.	8.1	More Details
CVE-2025-69399	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Cobble cobble allows PHP Local File Inclusion.This issue affects Cobble: from n/a through <= 1.7.	8.1	More Details
CVE-2025-69398	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Plank plank allows PHP Local File Inclusion.This issue affects Plank: from n/a through <= 1.7.	8.1	More Details
CVE-2025-69374	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SolverWp Eleblog – Elementor Blog And Magazine Addons ele-blog allows PHP Local File Inclusion.This issue affects Eleblog – Elementor Blog And Magazine Addons: from n/a through <= 2.0.3.	8.1	More Details
CVE-2025-69397	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Tint tint allows PHP Local File Inclusion.This issue affects Tint: from n/a through <= 1.7.	8.1	More Details
CVE-2026-27206	Zumba Json Serializer is a library to serialize PHP variables in JSON format. In versions 3.2.2 and below, the library allows deserialization of PHP objects from JSON using a special @type field. The deserializer instantiates any class specified in the @type field without restriction. When processing untrusted JSON input, this behavior may allow an attacker to instantiate arbitrary classes available in the application. If a vulnerable application passes attacker-controlled JSON into JsonSerializer::unserialize() and contains classes with dangerous magic methods (such as __wakeup() or __destruct()), this may lead to PHP Object Injection and potentially Remote Code Execution (RCE), depending on available gadget chains in the application or its dependencies. This behavior is similar in risk profile to PHP's native unserialize() when used without the allowed_classes restriction. Applications are impacted only if untrusted or attacker-controlled JSON is passed into JsonSerializer::unserialize() and the application or its dependencies contain classes that can be leveraged as a gadget chain. This issue has been fixed in version 3.2.3. If an immediate upgrade isn't feasible, mitigate the vulnerability by never deserializing untrusted JSON with JsonSerializer::unserialize(), validating and sanitizing all JSON input before deserialization, and disabling @type-based object instantiation wherever possible.	8.1	More Details
CVE-2025-69396	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Splendour splendour allows PHP Local File Inclusion.This issue affects Splendour: from n/a through <= 1.23.	8.1	More Details
CVE-2026-22367	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Coworking coworking allows PHP Local File Inclusion.This issue affects Coworking: from n/a through <= 1.6.1.	8.1	More Details
CVE-2026-22374	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Zio Alberto zioalberto allows PHP Local File Inclusion.This issue affects Zio Alberto: from n/a through <= 1.2.2.	8.1	More Details
CVE-2026-22368	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Redy redy allows PHP Local File Inclusion.This issue affects Redy: from n/a through <= 1.0.2.	8.1	More Details

CVE-2026-22369	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Ironfit ironfit allows PHP Local File Inclusion.This issue affects Ironfit: from n/a through <= 1.5.	8.1	More Details
CVE-2026-22376	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Parkivia parkivia allows PHP Local File Inclusion.This issue affects Parkivia: from n/a through <= 1.1.9.	8.1	More Details
CVE-2026-22377	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Saveo saveo allows PHP Local File Inclusion.This issue affects Saveo: from n/a through <= 1.1.2.	8.1	More Details
CVE-2025-68543	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Diza diza allows PHP Local File Inclusion.This issue affects Diza: from n/a through <= 1.3.15.	8.1	More Details
CVE-2025-68539	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Fana fana allows PHP Local File Inclusion.This issue affects Fana: from n/a through <= 1.1.35.	8.1	More Details
CVE-2026-22378	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Blabber blabber allows PHP Local File Inclusion.This issue affects Blabber: from n/a through <= 1.7.0.	8.1	More Details
CVE-2025-68536	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Zota zota allows PHP Local File Inclusion.This issue affects Zota: from n/a through <= 1.3.14.	8.1	More Details
CVE-2026-22379	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Netmix netmix allows PHP Local File Inclusion.This issue affects Netmix: from n/a through <= 1.0.10.	8.1	More Details
CVE-2026-26362	Dell Unisphere for PowerMax, version(s) 10.2, contain(s) a Relative Path Traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized modification of critical system files.	8.1	More Details
CVE-2026-26360	Dell Unisphere for PowerMax, version(s) 10.2, contain(s) an External Control of File Name or Path vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability to delete arbitrary files.	8.1	More Details
CVE-2026-22380	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes UnlimHost unlimhost allows PHP Local File Inclusion.This issue affects UnlimHost: from n/a through <= 1.2.3.	8.1	More Details
CVE-2026-22381	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes PawFriends - Pet Shop and Veterinary WordPress Theme pawfriends allows PHP Local File Inclusion.This issue affects PawFriends - Pet Shop and Veterinary WordPress Theme: from n/a through <= 1.3.	8.1	More Details
CVE-2025-67992	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in LoftOcean PatioTime patiotime allows PHP Local File Inclusion.This issue affects PatioTime: from n/a through < 2.1.	8.1	More Details
CVE-2025-67988	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in LoftOcean CozyStay cozystay allows PHP Local File Inclusion.This issue affects CozyStay: from n/a through < 1.9.1.	8.1	More Details
CVE-2025-67982	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Urna urna allows PHP Local File Inclusion.This issue affects Urna: from n/a through <= 2.5.12.	8.1	More Details
CVE-2025-67981	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Besa besa allows PHP Local File Inclusion.This issue affects Besa: from n/a through <= 2.3.15.	8.1	More Details
CVE-2026-26016	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to version 1.12.1, a missing authorization check in multiple controllers allows any user with access to a node secret token to fetch information about any server on a Pterodactyl instance, even if that server is associated with a different node. This issue stems from missing logic to verify that the node requesting server data is the same node that the server is associated with. Any authenticated Wings node can retrieve server installation scripts (potentially containing secret values) and manipulate the installation status of servers belonging to other nodes. Wings nodes may also manipulate the transfer status of servers belonging to other nodes. This vulnerability requires a user to acquire a secret access token for a node. Unless a user gains access to a Wings secret access token they would not be able to access any of these vulnerable endpoints, as every endpoint requires a valid node access token. A single compromised Wings node daemon token (stored in plaintext at `/etc/pterodactyl/config.yml`) grants access to sensitive configuration data of every server on the panel, rather than only to servers that the node has access to. An attacker can use this information to move laterally through the system, send excessive notifications, destroy server data on other nodes, and otherwise exfiltrate secrets that they should not have access to with only a node token. Additionally, triggering a false transfer success causes the panel to delete the server from the source node, resulting in permanent data loss. Users should upgrade to version 1.12.1 to receive a fix.	8.1	More Details
CVE-2026-20761	A vulnerability exists in EnOcean SmartServer IoT version 4.60.009 and prior, which would allow remote attackers, in the LON IP-852 management messages, to send specially crafted IP-852 messages resulting in arbitrary OS command execution on the device.	8.1	More Details

CVE-2026-22344	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes FiveStar fivestar allows PHP Local File Inclusion.This issue affects FiveStar: from n/a through <= 1.7.	8.1	More Details
CVE-2026-22373	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Fooddy fooddy allows PHP Local File Inclusion.This issue affects Fooddy: from n/a through <= 1.3.10.	8.1	More Details
CVE-2026-22371	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Gustavo gustavo allows PHP Local File Inclusion.This issue affects Gustavo: from n/a through <= 1.2.2.	8.1	More Details
CVE-2025-69322	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes PeakShops peakshops allows PHP Local File Inclusion.This issue affects PeakShops: from n/a through < 1.5.9.	8.1	More Details
CVE-2026-22370	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Marveland marveland allows PHP Local File Inclusion.This issue affects Marveland: from n/a through <= 1.3.0.	8.1	More Details
CVE-2026-25755	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.2.0, user control of the argument of the `addJS` method allows an attacker to inject arbitrary PDF objects into the generated document. By crafting a payload that escapes the JavaScript string delimiter, an attacker can execute malicious actions or alter the document structure, impacting any user who opens the generated PDF. The vulnerability has been fixed in jspdf@4.2.0. As a workaround, escape parentheses in user-provided JavaScript code before passing them to the `addJS` method.	8.1	More Details
CVE-2026-27190	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.6.8, a command injection vulnerability exists in Deno's node:child_process implementation. This vulnerability is fixed in 2.6.8.	8.1	More Details
CVE-2026-22372	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Isida isida allows PHP Local File Inclusion.This issue affects Isida: from n/a through <= 1.4.2.	8.1	More Details
CVE-2026-25940	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.2.0, user control of properties and methods of the Acroform module allows users to inject arbitrary PDF objects, such as JavaScript actions. If given the possibility to pass unsanitized input to one of the following property, a user can inject arbitrary PDF objects, such as JavaScript actions, which are executed when the victim hovers over the radio option. The vulnerability has been fixed in jsPDF@4.2.0. As a workaround, sanitize user input before passing it to the vulnerable API members.	8.1	More Details
CVE-2026-22375	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Impacto Patronus impacto-patronus allows PHP Local File Inclusion.This issue affects Impacto Patronus: from n/a through <= 1.2.3.	8.1	More Details
CVE-2026-22267	Dell PowerProtect Data Manager, version(s) prior to 19.22, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	8.1	More Details
CVE-2025-33245	NVIDIA NeMo Framework contains a vulnerability where malicious data could cause remote code execution. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	8.0	More Details
CVE-2026-27099	Jenkins 2.483 through 2.550 (both inclusive), LTS 2.492.1 through 2.541.1 (both inclusive) does not escape the user-provided description of the "Mark temporarily offline" offline cause, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure or Agent/Disconnect permission.	8.0	More Details
CVE-2025-33179	NVIDIA Cumulus Linux and NVOS products contain a vulnerability in the NVUE interface, where a low-privileged user could run an unauthorized command. A successful exploit of this vulnerability might lead to escalation of privileges.	8.0	More Details
CVE-2025-70329	TOTOLink X5000R v9.1.0cu_2415_B20250515 contains an OS command injection vulnerability in the setIptvCfg handler of the /usr/sbin/lighttpd executable. The vlanVidLan1 (and other vlanVidLanX) parameters are retrieved via Uci_Get_Str and passed to the CsteSystem function without adequate validation or filtering. This allows an authenticated attacker to execute arbitrary shell commands with root privileges by injecting shell metacharacters into the affected parameters.	8.0	More Details
CVE-2025-33180	NVIDIA Cumulus Linux and NVOS products contain a vulnerability in the NVUE interface, where a low-privileged user could inject a command. A successful exploit of this vulnerability might lead to escalation of privileges.	8.0	More Details
CVE-2019-25435	Sricam DeviceViewer 3.12.0.1 contains a local buffer overflow vulnerability in the user management add user function that allows authenticated attackers to execute arbitrary code by bypassing data execution prevention. Attackers can inject a malicious payload through the Username field in User Management to trigger a stack-based buffer overflow and execute commands via ROP chain gadgets.	7.8	More Details
CVE-2025-33243	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution in distributed environments. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-33241	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution by loading a maliciously crafted file. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details

CVE-2026-23599	A local privilege-escalation vulnerability has been discovered in the HPE Aruba Networking ClearPass OnGuard Software for Linux. Successful exploitation of this vulnerability could allow a local attacker to achieve arbitrary code execution with root privileges.	7.8	More Details
CVE-2025-4960	The com.epson.InstallNavi.helper tool, deployed with the EPSON printer driver installer, contains a local privilege escalation vulnerability due to multiple flaws in its implementation. It fails to properly authenticate clients over the XPC protocol and does not correctly enforce macOS's authorization model, exposing privileged functionality to untrusted users. Although it invokes the AuthorizationCopyRights API, it does so using overly permissive custom rights that it registers in the system's authorization database (/var/db/auth.db). These rights can be requested and granted by the authorization daemon to any local user, regardless of privilege level. As a result, an attacker can exploit the vulnerable service to perform privileged operations such as executing arbitrary commands or installing system components without requiring administrative credentials.	7.8	More Details
CVE-2025-33246	NVIDIA NeMo Framework for all platforms contains a vulnerability in the ASR Evaluator utility, where a user could cause a command injection by supplying crafted input to a configuration parameter. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, or information disclosure.	7.8	More Details
CVE-2026-26200	HDF5 is software for managing data. Prior to version 1.14.4-2, an attacker who can control an `h5` file parsed by HDF5 can trigger a write-based heap buffer overflow condition. This can lead to a denial-of-service condition, and potentially further issues such as remote code execution depending on the practical exploitability of the heap overflow against modern operating systems. Real-world exploitability of this issue in terms of remote-code execution is currently unknown. Version 1.14.4-2 fixes the issue.	7.8	More Details
CVE-2025-33240	NVIDIA Megatron Bridge contains a vulnerability in a data shuffling tutorial, where malicious input could cause a code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-33236	NVIDIA NeMo Framework contains a vulnerability where malicious data created by an attacker could cause code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-60035	A vulnerability has been identified in the OPC.Testclient utility, which is included in Rexroth IndraWorks. All versions prior to 15V24 are affected. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running the OPC.Testclient.	7.8	More Details
CVE-2026-27001	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, OpenClaw embedded the current working directory (workspace path) into the agent system prompt without sanitization. If an attacker can cause OpenClaw to run inside a directory whose name contains control/format characters (for example newlines or Unicode bidi/zero-width markers), those characters could break the prompt structure and inject attacker-controlled instructions. Starting in version 2026.2.15, the workspace path is sanitized before it is embedded into any LLM prompt output, stripping Unicode control/format characters and explicit line/paragraph separators. Workspace path resolution also applies the same sanitization as defense-in-depth.	7.8	More Details
CVE-2026-0874	A maliciously crafted CATPART file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-33251	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-27212	Swiper is a free and mobile touch slider with hardware accelerated transitions and native behavior. Versions 6.5.1 through 12.1.1 have a Prototype pollution vulnerability. The vulnerability resides in line 94 of shared/utils.mjs, where the indexOf() function is used to check whether user provided input contain forbidden strings. Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using Array.prototype. The exploit works across Windows and Linux and on Node and Bun runtimes. Any application that processes attacker-controlled input using this package may be affected by the following: Authentication Bypass, Denial of Service and RCE. This issue is fixed in version 12.1.2.	7.8	More Details
CVE-2025-33252	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2025-15561	An attacker can exploit the update behavior of the WorkTime monitoring daemon to elevate privileges on the local system to NT Authority\SYSTEM. A malicious executable must be named WTWatch.exe and dropped in the C:\ProgramData\wta\ClientExe directory, which is writable by "Everyone". The executable will then be run by the WorkTime monitoring daemon.	7.8	More Details
CVE-2025-33253	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution by convincing a user to load a maliciously crafted file. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-26959	ADB Explorer is a fluent UI for ADB on Windows. Versions 0.9.26020 and below fail to validate the integrity or authenticity of the ADB binary path specified in the ManualAdbPath setting before executing it, allowing arbitrary code execution with the privileges of the current user. An attacker can exploit this by crafting a malicious App.txt settings file that points ManualAdbPath to an arbitrary executable, then convincing a victim to launch the application with a command-line argument directing it to the malicious configuration directory. This vulnerability could be leveraged through social engineering tactics, such as distributing a shortcut bundled with a crafted settings file in an archive, resulting in RCE upon application startup. Thus issue has been fixed in version 0.9.26021.	7.8	More Details
CVE-2025-33239	NVIDIA Megatron Bridge contains a vulnerability in a data merging tutorial, where malicious input could cause a code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details

CVE-2026-0875	A maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-33250	NVIDIA NeMo Framework contains a vulnerability where an attacker could cause remote code execution. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2025-60036	A vulnerability has been identified in the UA.Testclient utility, which is included in Rexroth IndraWorks. All versions prior to 15V24 are affected. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running the UA.Testclient.	7.8	More Details
CVE-2025-60037	A vulnerability has been identified in Rexroth IndraWorks. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running Rexroth IndraWorks.	7.8	More Details
CVE-2025-60038	A vulnerability has been identified in Rexroth IndraWorks. This flaw allows an attacker to execute arbitrary code on the user's system by parsing a manipulated file containing malicious serialized data. Exploitation requires user interaction, specifically opening a specially crafted file, which then causes the application to deserialize the malicious data, enabling Remote Code Execution (RCE). This can lead to a complete compromise of the system running Rexroth IndraWorks.	7.8	More Details
CVE-2025-33249	NVIDIA NeMo Framework for all platforms contains a vulnerability in a voice-preprocessing script, where malicious input created by an attacker could cause a code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-2998	ERP developed by eAI Technologies has a DLL Hijacking vulnerability, allowing authenticated local attackers to place a crafted DLL file in the same directory as the program, thereby executing arbitrary code.	7.8	More Details
CVE-2025-61982	An arbitrary code execution vulnerability exists in the Code Stream directive functionality of OpenCFD OpenFOAM 2506. A specially crafted OpenFOAM simulation file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2024-1524	When the "Silent Just-In-Time Provisioning" feature is enabled for a federated identity provider (IDP) there is a risk that a local user store user's information may be replaced during the account provisioning process in cases where federated users share the same username as local users. There will be no impact on your deployment if any of the preconditions mentioned below are not met. Only when all the preconditions mentioned below are fulfilled could a malicious actor associate a targeted local user account with a federated IDP user account that they control. The Deployment should have: -An IDP configured for federated authentication with Silent JIT provisioning enabled. The malicious actor should have: -A fresh valid user account in the federated IDP that has not been used earlier. -Knowledge of the username of a valid user in the local IDP. -An account at the federated IDP matching the targeted local username.	7.7	More Details
CVE-2026-27479	Wallos is an open-source, self-hostable personal subscription tracker. Versions 4.6.0 and below contain a Server-Side Request Forgery (SSRF) vulnerability in the subscription and payment logo/icon upload functionality. The application validates the IP address of the provided URL before making the request, but allows HTTP redirects (CURLOPT_FOLLOWLOCATION = true), enabling an attacker to bypass the IP validation and access internal resources, including cloud instance metadata endpoints. The getLogoFromUrl() function validates the URL by resolving the hostname and checking if the resulting IP is in a private or reserved range using FILTER_FLAG_NO_PRIV_RANGE | FILTER_FLAG_NO_RES_RANGE. However, the subsequent cURL request is configured with CURLOPT_FOLLOWLOCATION = true and CURLOPT_MAXREDIRS = 3, which means the request will follow HTTP redirects without re-validating the destination IP. This issue has been fixed in version 4.6.1.	7.7	More Details
CVE-2025-1272	The Linux Kernel lockdown mode for kernel versions starting on 6.12 and above for Fedora Linux has the lockdown mode disabled without any warning. This may allow an attacker to gain access to sensitive information such kernel memory mappings, I/O ports, BPF and kprobes. Additionally unsigned modules can be loaded, leading to execution of untrusted code breaking breaking any Secure Boot protection. This vulnerability affects only Fedora Linux.	7.7	More Details
CVE-2026-27464	Metabase is an open-source data analytics platform. In versions prior to 0.57.13 and versions 0.58.x through 0.58.6, authenticated users are able to retrieve sensitive information from a Metabase instance, including database access credentials. During testing, it was confirmed that a low-privileged user can extract sensitive information including database credentials, into the email body via template evaluation. This issue has been fixed in versions 0.57.13 and 0.58.7. To workaround this issue, users can disable notifications in their Metabase instance to disallow access to the vulnerable endpoints.	7.7	More Details
CVE-2026-27487	OpenClaw is a personal AI assistant. In versions 2026.2.13 and below, when using macOS, the Claude CLI keychain credential refresh path constructed a shell command to write the updated JSON blob into Keychain via security add-generic-password -w .... Because OAuth tokens are user-controlled data, this created an OS command injection risk. This issue has been fixed in version 2026.2.14.	7.6	More Details
CVE-2026-26724	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v. 20230721a allows a remote attacker to execute arbitrary code via the selectgroup and gn parameters on the /?Function=Groups endpoint.	7.6	More Details
CVE-2026-25418	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in bitpressadmin Bit Form bit-form allows SQL Injection.This issue affects Bit Form: from n/a through <= 2.21.10.	7.6	More Details
	Fabric.js is a Javascript HTML5 canvas library. Prior to version 7.2.0, Fabric.js applies `escapeXml()` to text content during SVG export (`src/shapes/Text/TextSVGExportMixin.ts:186`) but fails to apply it to other user-controlled string values that are interpolated into SVG attribute markup. When attacker-controlled JSON is loaded via `loadFromJSON()` and later exported via		

CVE-2026-27013	`toSVG()`, the unescaped values break out of XML attributes and inject arbitrary SVG elements including event handlers. Any application that accepts user-supplied JSON (via `loadFromJSON()`, collaborative sharing, import features, CMS plugins) and renders the `toSVG()` output in a browser context (SVG preview, export download rendered in-page, email template, embed) is vulnerable to stored XSS. An attacker can execute arbitrary JavaScript in the victim's browser session. Version 7.2.0 contains a fix.	7.6	More Details
CVE-2026-25802	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to version 0.10.8-alpha.9, a potential unsafe operation occurs in component `MarkdownRenderer.jsx`, allowing for Cross-Site Scripting(XSS) when the model outputs items containing `<script>` tag. Version 0.10.8-alpha.9 fixes the issue.	7.6	More Details
CVE-2026-22567	Improper validation of user-supplied input in the ZIA Admin UI could allow an authenticated administrator to initiate backend functions through specific input fields in limited scenarios.	7.6	More Details
CVE-2026-25378	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nelio Software Nelio AB Testing nelio-ab-testing allows Blind SQL Injection.This issue affects Nelio AB Testing: from n/a through <= 8.2.4.	7.6	More Details
CVE-2026-23805	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yoren Chang Media Search Enhanced media-search-enhanced allows SQL Injection.This issue affects Media Search Enhanced: from n/a through <= 0.9.1.	7.6	More Details
CVE-2026-26322	OpenClaw is a personal AI assistant. Prior to OpenClaw version 2026.2.14, the Gateway tool accepted a tool-supplied `gatewayUrl` without sufficient restrictions, which could cause the OpenClaw host to attempt outbound WebSocket connections to user-specified targets. This requires the ability to invoke tools that accept `gatewayUrl` overrides (directly or indirectly). In typical setups this is limited to authenticated operators, trusted automation, or environments where tool calls are exposed to non-operators. In other words, this is not a drive-by issue for arbitrary internet users unless a deployment explicitly allows untrusted users to trigger these tool calls. Some tool call paths allowed `gatewayUrl` overrides to flow into the Gateway WebSocket client without validation or allowlisting. This meant the host could be instructed to attempt connections to non-gateway endpoints (for example, localhost services, private network addresses, or cloud metadata IPs). In the common case, this results in an outbound connection attempt from the OpenClaw host (and corresponding errors/timeouts). In environments where the tool caller can observe the results, this can also be used for limited network reachability probing. If the target speaks WebSocket and is reachable, further interaction may be possible. Starting in version 2026.2.14, tool-supplied `gatewayUrl` overrides are restricted to loopback (on the configured gateway port) or the configured `gateway.remote.url`. Disallowed protocols, credentials, query/hash, and non-root paths are rejected.	7.6	More Details
CVE-2026-3105	SummaryThis advisory addresses a SQL injection vulnerability in the API endpoint used for retrieving contact activities. A vulnerability exists in the query construction for the Contact Activity timeline where the parameter responsible for determining the sort direction was not strictly validated against an allowlist, potentially allowing authenticated users to inject arbitrary SQL commands via the API. MitigationPlease update to 4.4.19, 5.2.10, 6.0.8, 7.0.1 or later. WorkaroundsNone. ReferencesIf you have any questions or comments about this advisory: Email us at security@mautic.org	7.6	More Details
CVE-2026-26202	Penpot is an open-source design tool for design and code collaboration. Prior to version 2.13.2, an authenticated user can read arbitrary files from the server by supplying a local file path (e.g. `/etc/passwd`) as a font data chunk in the `create-font-variant` RPC endpoint, resulting in the file contents being stored and retrievable as a "font" asset. This is an arbitrary file read vulnerability. Any authenticated user with team edit permissions can read arbitrary files accessible to the Penpot backend process on the host filesystem. This can lead to exposure of sensitive system files, application secrets, database credentials, and private keys, potentially enabling further compromise of the server. In containerized deployments, the blast radius may be limited to the container filesystem, but environment variables, mounted secrets, and application configuration are still at risk. Version 2.13.2 contains a patch for the issue.	7.5	More Details
CVE-2026-24941	Missing Authorization vulnerability in wpjobportal WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through <= 2.4.4.	7.5	More Details
CVE-2026-22356	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Automattic Jetpack CRM zero-bs-crm allows PHP Local File Inclusion.This issue affects Jetpack CRM: from n/a through <= 6.7.0.	7.5	More Details
CVE-2026-25998	strongMan is a management interface for strongSwan, an OpenSource IPsec-based VPN. When storing credentials in the database (private keys, EAP secrets), strongMan encrypts the corresponding database fields. So far it used AES in CTR mode with a global database key. Together with an initialization vector (IV), a key stream is generated to encrypt the data in the database fields. But because strongMan did not generate individual IVs, every database field was encrypted using the same key stream. An attacker that has access to the database can use this to recover the encrypted credentials. In particular, because certificates, which have to be considered public information, are also encrypted using the same mechanism, an attacker can directly recover a large chunk of the key stream, which allows them to decrypt basically all other secrets especially ECDSA private keys and EAP secrets, which are usually a lot shorter. Version 0.2.0 fixes the issue by switching to AES-GCM-SIV encryption with a random nonce and an individually derived encryption key, using HKDF, for each encrypted value. Database migrations are provided to automatically re-encrypt all credentials.	7.5	More Details
CVE-2025-68841	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Themepul TopperPack – Complete Elementor Addons, Theme & CPT Builder topper-pack allows PHP Local File Inclusion.This issue affects TopperPack – Complete Elementor Addons, Theme & CPT Builder: from n/a through <= 1.2.1.	7.5	More Details
CVE-2026-26996	minimatch is a minimal matching utility for converting glob expressions into JavaScript RegExp objects. Versions 10.2.0 and below are vulnerable to Regular Expression Denial of Service (ReDoS) when a glob pattern contains many consecutive * wildcards followed by a literal character that doesn't appear in the test string. Each * compiles to a separate [^/]*? regex group, and when the match fails, V8's regex engine backtracks exponentially across all possible splits. The time complexity is O(4^N) where N is the number of * characters. With N=15, a single minimatch() call takes ~2 seconds. With N=34, it hangs effectively forever. Any application that passes user-controlled strings to minimatch() as the pattern argument is vulnerable to DoS. This issue has been fixed in version 10.2.1.	7.5	More Details

CVE-2026-27052	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in villatheme Sales Countdown Timer for WooCommerce and WordPress sctv-sales-countdown-timer allows PHP Local File Inclusion.This issue affects Sales Countdown Timer for WooCommerce and WordPress: from n/a through <= 1.1.8.1.	7.5	More Details
CVE-2026-26267	soroban-sdk is a Rust SDK for Soroban contracts. Prior to versions 22.0.10, 23.5.2, and 25.1.1, the `#[contractimpl]` macro contains a bug in how it wires up function calls. `#[contractimpl]` generates code that uses `MyContract::value()` style calls even when it's processing the trait version. This means if an inherent function is also defined with the same name, the inherent function gets called instead of the trait function. This means the Wasm-exported entry point silently calls the wrong function when two conditions are met simultaneously: First, an `impl Trait for MyContract` block is defined with one or more functions, with `#[contractimpl]` applied. Second, an `impl MyContract` block is defined with one or more identically named functions, without `#[contractimpl]` applied. If the trait version contains important security checks, such as verifying the caller is authorized, that the inherent version does not, those checks are bypassed. Anyone interacting with the contract through its public interface will call the wrong function. The problem is patched in `soroban-sdk-macros` versions 22.0.10, 23.5.2, and 25.1.1. The fix changes the generated call from `<Type>::func()` to `<Type as Trait>::func()` when processing trait implementations, ensuring Rust resolves to the trait associated function regardless of whether an inherent function with the same name exists. Users should upgrade to `soroban-sdk-macros` 22.0.10, 23.5.2, or 25.1.1 and recompile their contracts. If upgrading is not immediately possible, contract developers can avoid the issue by ensuring that no inherent associated function on the contract type shares a name with any function in the trait implementation. Renaming or removing the conflicting inherent function eliminates the ambiguity and causes the macro-generated code to correctly resolve to the trait function.	7.5	More Details
CVE-2025-67974	Missing Authorization vulnerability in WP Legal Pages WPLegalPages wplegalpages allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPLegalPages: from n/a through <= 3.5.4.	7.5	More Details
CVE-2026-26278	fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. In versions 4.1.3 through 5.3.5, the XML parser can be forced to do an unlimited amount of entity expansion. With a very small XML input, it’s possible to make the parser spend seconds or even minutes processing a single request, effectively freezing the application. Version 5.3.6 fixes the issue. As a workaround, avoid using DOCTYPE parsing by `processEntities: false` option.	7.5	More Details
CVE-2026-22383	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes PawFriends - Pet Shop and Veterinary WordPress Theme pawfriends allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PawFriends - Pet Shop and Veterinary WordPress Theme: from n/a through <= 1.3.	7.5	More Details
CVE-2025-69393	Missing Authorization vulnerability in Jthemes Exzo exzo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Exzo: from n/a through <= 1.2.4.	7.5	More Details
CVE-2026-25474	OpenClaw is a personal AI assistant. In versions 2026.1.30 and below, if channels.telegram.webhookSecret is not set when in Telegram webhook mode, OpenClaw may accept webhook HTTP requests without verifying Telegram’s secret token header. In deployments where the webhook endpoint is reachable by an attacker, this can allow forged Telegram updates (for example spoofing message.from.id). If an attacker can reach the webhook endpoint, they may be able to send forged updates that are processed as if they came from Telegram. Depending on enabled commands/tools and configuration, this could lead to unintended bot actions. Note: Telegram webhook mode is not enabled by default. It is enabled only when `channels.telegram.webhookUrl` is configured. This issue has been fixed in version 2026.2.1.	7.5	More Details
CVE-2026-26336	Hyland Alfresco allows unauthenticated attackers to read arbitrary files from protected directories (like WEB-INF) via the "/share/page/resource/" endpoint, thus leading to the disclosure of sensitive configuration files.	7.5	More Details
CVE-2026-26321	OpenClaw is a personal AI assistant. Prior to OpenClaw version 2026.2.14, the Feishu extension previously allowed `sendMediaFeishu` to treat attacker-controlled `mediaUrl` values as local filesystem paths and read them directly. If an attacker can influence tool calls (directly or via prompt injection), they may be able to exfiltrate local files by supplying paths such as `/etc/passwd` as `mediaUrl`. Upgrade to OpenClaw `2026.2.14` or newer to receive a fix. The fix removes direct local file reads from this path and routes media loading through hardened helpers that enforce local-root restrictions.	7.5	More Details
CVE-2026-26275	httpsig-hyper is a hyper extension for http message signatures. An issue was discovered in `httpsig-hyper` prior to version 0.0.23 where Digest header verification could incorrectly succeed due to misuse of Rust's `matches!` macro. Specifically, the comparison `if matches!(digest, _expected_digest)` treated `_expected_digest` as a pattern binding rather than a value comparison, resulting in unconditional success of the match expression. As a consequence, digest verification could incorrectly return success even when the computed digest did not match the expected value. Applications relying on Digest verification as part of HTTP message signature validation may therefore fail to detect message body modification. The severity depends on how the library is integrated and whether additional signature validation layers are enforced. This issue has been fixed in `httpsig-hyper` 0.0.23. The fix replaces the incorrect `matches!` usage with proper value comparison and additionally introduces constant-time comparison for digest verification as defense-in-depth. Regression tests have also been added to prevent reintroduction of this issue. Users are strongly advised to upgrade to the patched version. There is no reliable workaround without upgrading. Users who cannot immediately upgrade should avoid relying solely on Digest verification for message integrity and ensure that full HTTP message signature verification is enforced at the application layer.	7.5	More Details
CVE-2026-27114	NanaZip is an open source file archive Starting in version 5.0.1252.0 and prior to version 6.0.1630.0, circular `NextOffset` chains cause an infinite loop in the ROMFS archive parser. Version 6.0.1630.0 patches the issue.	7.5	More Details
CVE-2026-26313	go-ethereum (geth) is a golang execution layer implementation of the Ethereum protocol. Prior to version 1.17.0, an attacker can cause high memory usage by sending a specially-crafted p2p message. The issue is resolved in the v1.17.0 release.	7.5	More Details
CVE-2026-26314	go-ethereum (geth) is a golang execution layer implementation of the Ethereum protocol. Prior to version 1.16.9, a vulnerable node can be forced to shutdown/crash using a specially crafted message. The problem is resolved in the v1.16.9 and v1.17.0 releases of Geth.	7.5	More Details

CVE-2026-26315	go-ethereum (Geth) is a golang execution layer implementation of the Ethereum protocol. Prior to version 1.16.9, through a flaw in the ECIES cryptography implementation, an attacker may be able to extract bits of the p2p node key. The issue is resolved in the v1.16.9 and v1.17.0 releases of Geth. Geth maintainers recommend rotating the node key after applying the upgrade, which can be done by removing the file `<datadir>/geth/nodekey` before starting Geth.	7.5	More Details
CVE-2026-26316	OpenClaw is a personal AI assistant. Prior to 2026.2.13, the optional BlueBubbles iMessage channel plugin could accept webhook requests as authenticated based only on the TCP peer address being loopback (`127.0.0.1`, `::1`, `::ffff:127.0.0.1`) even when the configured webhook secret was missing or incorrect. This does not affect the default iMessage integration unless BlueBubbles is installed and enabled. Version 2026.2.13 contains a patch. Other mitigations include setting a non-empty BlueBubbles webhook password and avoiding deployments where a public-facing reverse proxy forwards to a loopback-bound Gateway without strong upstream authentication.	7.5	More Details
CVE-2026-26319	OpenClaw is a personal AI assistant. Versions 2026.2.13 and below allow the optional @openclaw/voice-call plugin Telnyx webhook handler to accept unsigned inbound webhook requests when telnyx.publicKey is not configured, enabling unauthenticated callers to forge Telnyx events. Telnyx webhooks are expected to be authenticated via Ed25519 signature verification. In affected versions, TelnyxProvider.verifyWebhook() could effectively fail open when no Telnyx public key was configured, allowing arbitrary HTTP POST requests to the voice-call webhook endpoint to be treated as legitimate Telnyx events. This only impacts deployments where the Voice Call plugin is installed, enabled, and the webhook endpoint is reachable from the attacker (for example, publicly exposed via a tunnel/proxy). The issue has been fixed in version 2026.2.14.	7.5	More Details
CVE-2025-69373	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in beeteam368 VidoRev vidorev allows PHP Local File Inclusion.This issue affects VidoRev: from n/a through <= 2.9.9.9.9.9.7.	7.5	More Details
CVE-2026-27343	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in VanKarWai Airtifact airtifact allows PHP Local File Inclusion.This issue affects Airtifact: from n/a through <= 1.2.91.	7.5	More Details
CVE-2025-69380	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vanquish Upload Files Anywhere wp-upload-files-anywhere allows Path Traversal.This issue affects Upload Files Anywhere: from n/a through <= 2.8.	7.5	More Details
CVE-2025-69297	Missing Authorization vulnerability in GhostPool Aardvark Plugin aardvark-plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Aardvark Plugin: from n/a through <= 2.19.	7.5	More Details
CVE-2025-69383	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Agence web Eoxia - Montpellier WP shop wpshop allows PHP Local File Inclusion.This issue affects WP shop: from n/a through <= 2.6.1.	7.5	More Details
CVE-2025-69387	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in whatwouldjessedo Simple Retail Menus simple-retail-menus allows PHP Local File Inclusion.This issue affects Simple Retail Menus: from n/a through <= 4.2.1.	7.5	More Details
CVE-2026-25326	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in cmsmasters CMSMasters Content Composer cmsmasters-content-composer allows PHP Local File Inclusion.This issue affects CMSMasters Content Composer: from n/a through <= 1.4.5.	7.5	More Details
CVE-2026-2232	The Product Table and List Builder for WooCommerce Lite plugin for WordPress is vulnerable to time-based SQL Injection via the 'search' parameter in all versions up to, and including, 4.6.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-26324	OpenClaw is a personal AI assistant. Prior to version 2026.2.14, OpenClaw's SSRF protection could be bypassed using full-form IPv4-mapped IPv6 literals such as `0:0:0:0:0:ffff:7f00:1` (which is `127.0.0.1`). This could allow requests that should be blocked (loopback / private network / link-local metadata) to pass the SSRF guard. Version 2026.2.14 patches the issue.	7.5	More Details
CVE-2026-25535	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.2.0, user control of the first argument of the `addImage` method results in denial of service. If given the possibility to pass unsanitized image data or URLs to the `addImage` method, a user can provide a harmful GIF file that results in out of memory errors and denial of service. Harmful GIF files have large width and/or height entries in their headers, which lead to excessive memory allocation. Other affected methods are: `html`. The vulnerability has been fixed in jsPDF 4.2.0. As a workaround, sanitize image data or URLs before passing it to the addImage method or one of the other affected methods.	7.5	More Details
CVE-2026-1581	The wpForo Forum plugin for WordPress is vulnerable to time-based SQL Injection via the 'wpfob' parameter in all versions up to, and including, 2.4.14 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-70148	Missing authentication and authorization in print_membership_card.php in CodeAstro Membership Management System 1.0 allows unauthenticated attackers to access membership card data of arbitrary users via direct requests with a manipulated id parameter, resulting in insecure direct object reference (IDOR).	7.5	More Details
CVE-2025-11754	The GDPR Cookie Consent plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'gdpr/v1/settings' REST API endpoint in all versions up to, and including, 4.1.2. This makes it possible for unauthenticated attackers to retrieve sensitive plugin settings including API tokens, email addresses, account IDs, and site keys.	7.5	More Details
CVE-2019-25358	FileOptimizer 14.00.2524 contains a denial of service vulnerability that allows attackers to crash the application by manipulating the FileOptimizer32.ini configuration file. Attackers can overwrite the TempDirectory parameter with a 5000-character buffer to cause the application to crash when opening options.	7.5	More Details
	Valkey is a distributed key-value database. Prior to versions 9.0.2, 8.1.6, 8.0.7, and 7.2.12, a malicious actor with access to the		

CVE-2026-21863	Valkey clusterbus port can send an invalid packet that may cause an out bound read, which might result in the system crashing. The Valkey clusterbus packet processing code does not validate that a clusterbus ping extension packet is located within buffer of the clusterbus packet before attempting to read it. Versions 9.0.2, 8.1.6, 8.0.7, and 7.2.12 fix the issue. As an additional mitigation, don't expose the cluster bus connection directly to end users, and protect the connection with its own network ACLs.	7.5	More Details
CVE-2026-27623	Valkey is a distributed key-value database. Starting in version 9.0.0 and prior to version 9.0.3, a malicious actor with network access to Valkey can cause the system to abort by triggering an assertion. When processing incoming requests, the Valkey system does not properly reset the networking state after processing an empty request. A malicious actor can then send a request that the server incorrectly identifies as breaking server side invariants, which results in the server shutting down. Version 9.0.3 fixes the issue. As an additional mitigation, properly isolate Valkey deployments so that only trusted users have access.	7.5	More Details
CVE-2019-25434	SpotAuditor 5.3.1.0 contains a denial of service vulnerability that allows unauthenticated attackers to crash the application by submitting excessive data in the registration name field. Attackers can enter a large string of characters (5000 bytes or more) in the name field during registration to trigger an unhandled exception that crashes the application.	7.5	More Details
CVE-2026-2576	The Business Directory Plugin – Easy Listing Directories for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'payment' parameter in all versions up to, and including, 6.4.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-70147	Missing authentication in /admin/student.php and /admin/teacher.php in ProjectWorlds Online Time Table Generator 1.0 allows remote attackers to obtain sensitive information (including plaintext password field values) via direct HTTP GET requests to these endpoints without a valid session.	7.5	More Details
CVE-2026-2507	When BIG-IP AFM or BIG-IP DDoS is provisioned, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-27161	GetSimple CMS is a content management system. All versions of GetSimple CMS rely on .htaccess files to restrict access to sensitive directories such as /data/ and /backups/. If Apache AllowOverride is disabled (common in hardened or shared hosting environments), these protections are silently ignored, allowing unauthenticated attackers to list and download sensitive files including authorization.xml, which contains cryptographic salts and API keys. This issue does not have a fix at the time of publication.	7.5	More Details
CVE-2019-25363	WMV to AVI MPEG DVD WMV Convertor 4.6.1217 contains a buffer overflow vulnerability that allows attackers to crash the application by providing an oversized license input. Attackers can generate a 6000-byte payload and paste it into the 'License Name and License Code' field to trigger an application crash.	7.5	More Details
CVE-2026-25985	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a crafted SVG file containing an malicious element causes ImageMagick to attempt to allocate ~674 GB of memory, leading to an out-of-memory abort. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	7.5	More Details
CVE-2026-1368	The Video Conferencing with Zoom WordPress plugin before 4.6.6 contains an AJAX handler that has its nonce verification commented out, allowing unauthenticated attackers to generate valid Zoom SDK signatures for any meeting ID and retrieve the site's Zoom SDK key.	7.5	More Details
CVE-2026-23491	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. a path traversal vulnerability exists in the `get_file` method of the `Guest` module's `Get` controller in InvoicePlane up to and including through 1.6.3. The vulnerability allows unauthenticated attackers to read arbitrary files on the server by manipulating the input filename. This leads to the disclosure of sensitive information, including configuration files with database credentials. Version 1.6.4 fixes the issue.	7.5	More Details
CVE-2026-22860	Rack is a modular Ruby web server interface. Prior to versions 2.2.22, 3.1.20, and 3.2.5, `Rack::Directory`'s path check used a string prefix match on the expanded path. A request like `/../root_example/` can escape the configured root if the target path starts with the root string, allowing directory listing outside the intended root. Versions 2.2.22, 3.1.20, and 3.2.5 fix the issue.	7.5	More Details
CVE-2019-25401	Bematech (formerly Logic Controls, now Elgin) MP-4200 TH printer contains a denial of service vulnerability in the admin configuration page. Remote attackers can send crafted POST requests with malformed 'admin' and 'person' parameters to crash the printer's web service, causing a denial of service condition.	7.5	More Details
CVE-2026-24481	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap information disclosure vulnerability exists in ImageMagick's PSD (Adobe Photoshop) format handler. When processing a maliciously crafted PSD file containing ZIP-compressed layer data that decompresses to less than the expected size, uninitialized heap memory is leaked into the output image. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	7.5	More Details
CVE-2026-27181	MajorDoMo (aka Major Domestic Module) allows unauthenticated arbitrary module uninstallation through the market module. The market module's admin() method reads gr('mode') from $_REQUEST and assigns it to $this->mode at the start of execution, making all mode-gated code paths reachable without authentication via the /objects/?module=market endpoint. The uninstall mode handler calls uninstallPlugin(), which deletes module records from the database, executes the module's uninstall() method via eval(), recursively deletes the module's directory and template files using removeTree(), and removes associated cycle scripts. An attacker can iterate through module names and wipe the entire MajorDoMo installation with a series of unauthenticated GET requests.	7.5	More Details
CVE-2026-27202	GetSimple CMS is a content management system. All versions of GetSimple CMS have a flaw in the Uploaded Files feature that allows for arbitrary file reads. This issue has not been fixed at the time of publication.	7.5	More Details
CVE-2019-	Part-DB 0.4 contains an authentication bypass vulnerability that allows unauthenticated attackers to login by injecting SQL syntax into authentication parameters. Attackers can submit a single quote followed by 'or' in the login form to bypass	7.5	More Details

25432	credential validation and gain unauthorized access to the application.		
CVE-2019-25355	gSOAP 2.8 contains a directory traversal vulnerability that allows unauthenticated attackers to access system files by manipulating HTTP path traversal techniques. Attackers can retrieve sensitive files like /etc/passwd by sending crafted GET requests with multiple '../' directory traversal sequences.	7.5	More Details
CVE-2026-25989	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a crafted SVG file can cause a denial of service. An off-by-one boundary check (`>` instead of `>=`) that allows bypass the guard and reach an undefined `(size_t)` cast. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	7.5	More Details
CVE-2026-24892	openITCOCKPIT is an open source monitoring tool built for different monitoring engines like Nagios, Naemon and Prometheus. openITCOCKPIT Community Edition 5.3.1 and earlier contains an unsafe PHP deserialization pattern in the processing of changelog entries. Serialized changelog data derived from attacker-influenced application state is unserialized without restricting allowed classes. Although no current application endpoint was found to introduce PHP objects into this data path, the presence of an unrestricted unserialize() call constitutes a latent PHP object injection vulnerability. If future code changes, plugins, or refactors introduce object values into this path, the vulnerability could become immediately exploitable with severe impact, including potential remote code execution.	7.5	More Details
CVE-2026-25899	Fiber is an Express inspired web framework written in Go. In versions on the v3 branch prior to 3.1.0, the use of the `fiber_flash` cookie can force an unbounded allocation on any server. A crafted 10-character cookie value triggers an attempt to allocate up to 85GB of memory via unvalidated msgpack deserialization. No authentication is required. Every GoFiber v3 endpoint is affected regardless of whether the application uses flash messages. Version 3.1.0 fixes the issue.	7.5	More Details
CVE-2025-69700	Tenda FH1203 V2.0.1.6 contains a stack-based buffer overflow vulnerability in the modify_add_client_prio function, which is reachable via the formSetClientPrio CGI handler.	7.5	More Details
CVE-2026-24950	Authorization Bypass Through User-Controlled Key vulnerability in themeplugs Authorsy authorsy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Authorsy: from n/a through <= 1.0.6.	7.5	More Details
CVE-2026-24485	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, when a PCD file does not contain a valid Sync marker, the DecodeImage() function becomes trapped in an infinite loop while searching for the Sync marker, causing the program to become unresponsive and continuously consume CPU resources, ultimately leading to system resource exhaustion and denial of service. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	7.5	More Details
CVE-2026-27520	Binardat 10G08-0800GSM network switch firmware versions prior to V300SP10260209 store a user password in a client-side cookie as a Base64-encoded value accessible via the web interface. Because Base64 is reversible and provides no confidentiality, an attacker who can access the cookie value can recover the plaintext password.	7.5	More Details
CVE-2019-25349	ScadaApp for iOS 1.1.4.0 contains a denial of service vulnerability that allows attackers to crash the application by inputting an oversized buffer in the Servername field. Attackers can paste a 257-character buffer during login to trigger an application crash on iOS devices.	7.5	More Details
CVE-2019-25350	XMedia Recode 3.4.8.6 contains a denial of service vulnerability that allows attackers to crash the application by loading a specially crafted .m3u playlist file. Attackers can create a malicious .m3u file with an oversized buffer to trigger an application crash when the file is opened.	7.5	More Details
CVE-2019-25352	Crystal Live HTTP Server 6.01 contains a directory traversal vulnerability that allows remote attackers to access system files by manipulating URL path segments. Attackers can use multiple '../' sequences to navigate outside the web root and retrieve sensitive configuration files like Windows system files.	7.5	More Details
CVE-2026-24455	The embedded web interface of the device does not support HTTPS/TLS for authentication and uses HTTP Basic Authentication. Traffic is encoded but not encrypted, exposing user credentials to passive interception by attackers on the same network.	7.5	More Details
CVE-2026-26048	The Wi-Fi router is vulnerable to de-authentication attacks due to the absence of management frame protection, allowing forged deauthentication and disassociation frames to be broadcast without authentication or encryption. An attacker can use this to cause unauthorized disruptions and create a denial-of-service condition.	7.5	More Details
CVE-2026-27519	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior use RC4 with a hard-coded key embedded in client-side JavaScript. Because the key is static and exposed, an attacker can decrypt protected values and defeat confidentiality protections.	7.5	More Details
CVE-2019-25353	Foscam Video Management System 1.1.4.9 contains a denial of service vulnerability in the username input field that allows attackers to crash the application. Attackers can overwrite the username with a 520-byte buffer of repeated 'A' characters to trigger an application crash during device login.	7.5	More Details
CVE-2026-24891	openITCOCKPIT is an open source monitoring tool built for different monitoring engines like Nagios, Naemon and Prometheus. Versions 5.3.1 and below contain an unsafe deserialization sink in the Gearman worker implementation. The worker function registered as oitc_gearman calls PHP's unserialize() on job payloads without enforcing class restrictions or validating data origin. While the intended deployment assumes only trusted internal components enqueue Gearman jobs, this trust boundary is not enforced in application code. In environments where the Gearman service or worker is exposed to untrusted systems, an attacker may submit crafted serialized payloads to trigger PHP Object Injection in the worker process. This vulnerability is exploitable when Gearman listens on non-local interfaces, network access to TCP/4730 is unrestricted, or untrusted systems can enqueue jobs. Default, correctly hardened deployments may not be immediately exploitable, but the unsafe sink remains present in code regardless of deployment configuration. Enforcing this trust boundary in code would significantly reduce risk and prevent exploitation in misconfigured environments. This issue has been fixed in version 5.4.0.	7.5	More Details
CVE-2019-	iSmartViewPro 1.3.34 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the camera ID input field. Attackers can paste a 257-character buffer into the camera DID and password fields to trigger an	7.5	More

25354	application crash on iOS devices.		Details
CVE-2025-12707	The Library Management System plugin for WordPress is vulnerable to SQL Injection via the 'bid' parameter in all versions up to, and including, 3.2.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-2495	The WPNakama – Team and multi-Client Collaboration, Editorial and Project Management plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the '/wp-json/WPNakama/v1/boards' REST API endpoint in all versions up to, and including, 0.6.5. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-27579	CollabPlatform is a full-stack, real-time doc collaboration platform. In all versions of CollabPlatform, the Appwrite project used by the application is misconfigured to allow arbitrary origins in CORS responses while also permitting credentialed requests. An attacker-controlled domain can issue authenticated cross-origin requests and read sensitive user account information, including email address, account identifiers, and MFA status. The issue did not have a fix at the time of publication.	7.4	More Details
CVE-2026-25967	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-15, a stack-based buffer overflow exists in the ImageMagick FTXT image reader. A crafted FTXT file can cause out-of-bounds writes on the stack, leading to a crash. Version 7.1.2-15 contains a patch.	7.4	More Details
CVE-2026-25968	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a stack buffer overflow occurs when processing the an attribute in msl.c. A long value overflows a fixed-size stack buffer, leading to memory corruption. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	7.4	More Details
CVE-2025-63946	A privilege escalation (PE) vulnerability in the Tencent PC Manager app thru 17.10.28554.205 on Windows devices enables a local user to execute programs with elevated privileges. However, execution requires that the local user is able to successfully exploit a race condition.	7.4	More Details
CVE-2025-63945	A privilege escalation (PE) vulnerability in the Tencent iOA app thru 210.9.28693.621001 on Windows devices enables a local user to execute programs with elevated privileges. However, execution requires that the local user is able to successfully exploit a race condition.	7.4	More Details
CVE-2025-70045	An issue pertaining to CWE-295: Improper Certificate Validation was discovered in jxcore jxm master. The application disables TLS/SSL certificate validation by setting 'rejectUnauthorized': false in HTTPS request options when 'jx_obj.IsSecure' is true	7.4	More Details
CVE-2026-3042	A vulnerability was detected in itsourcecode Event Management System 1.0. The affected element is an unknown function of the file /admin/index.php. Performing a manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-2938	A vulnerability has been found in SourceCodester Student Result Management System 1.0. The affected element is an unknown function of the file /srms/script/admin/core/update_smtp.php. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9062	Authorization Bypass Through User-Controlled Key vulnerability in MeCODE Informatics and Engineering Services Ltd. Envanty allows Parameter Injection.This issue affects Envanty: before 1.0.6. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. The vulnerability was learned to be remediated through reporter information and testing.	7.3	More Details
CVE-2026-27488	OpenClaw is a personal AI assistant. In versions 2026.2.17 and below, Cron webhook delivery in src/gateway/server-cron.ts uses fetch() directly, so webhook targets can reach private/metadata/internal endpoints without SSRF policy checks. This issue was fixed in version 2026.2.19.	7.3	More Details
CVE-2026-2983	A vulnerability was determined in SourceCodester Student Result Management System 1.0. The impacted element is an unknown function of the file /admin/core/import_users.php of the component Bulk Import. This manipulation of the argument File causes improper access controls. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-3046	A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This vulnerability affects unknown code of the file /check_profile_old.php. The manipulation of the argument profile_id leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-2952	A flaw has been found in Vaelsys 4.1.0. This vulnerability affects unknown code of the file /tree/tree_server.php of the component HTTP POST Request Handler. This manipulation of the argument xajaxargs causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-21420	Dell Repository Manager (DRM), versions prior to 3.4.8, contains an Uncontrolled Search Path Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary code execution and escalation of privileges.	7.3	More Details
CVE-2026-2940	A vulnerability was determined in Zaher1307 tiny_web_server up to 8d77b1044a0ca3a5297d8726ac8aa2cf944d481b. This affects the function tiny_web_server/tiny.c of the file tiny_web_server/tiny.c of the component URL Handler. This manipulation causes out-of-bounds write. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2025-61144	libtiff up to v4.7.1 was discovered to contain a stack overflow via the readSeparateStripsIntoBuffer function.	7.3	More Details

CVE-2026-25649	Versions of the Traccar open-source GPS tracking system up to and including 6.11.1 contain an issue in which authenticated users can steal OAuth 2.0 authorization codes by exploiting an open redirect vulnerability in two OIDC-related endpoints. The `redirect_uri` parameter is not validated against a whitelist, allowing attackers to redirect authorization codes to attacker-controlled URLs, enabling account takeover on any OAuth-integrated application. As of time of publication, it is unclear whether a fix is available.	7.3	More Details
CVE-2026-2912	A vulnerability was found in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/students/assessments/results/studentresult-view.php. The manipulation of the argument test_id results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2821	A weakness has been identified in Fujian Smart Integrated Management Platform System up to 7.5. Impacted is an unknown function of the file /Module/CRXT/Controller/XCamera.ashx. This manipulation of the argument ChannelName causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-2867	A vulnerability was determined in itsourcecode Vehicle Management System 1.0. Affected is an unknown function of the file /billaction.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-2820	A security flaw has been discovered in Fujian Smart Integrated Management Platform System up to 7.5. This issue affects some unknown processing of the file /Module/CRXT/Controller/XAccessPermissionPlus.ashx. The manipulation of the argument DeviceIDS results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-2896	A weakness has been identified in funadmin up to 7.1.0-rc4. This affects the function setConfig of the file app/backend/controller/Ajax.php of the component Configuration Handler. Executing a manipulation can lead to improper authorization. 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.	7.3	More Details
CVE-2026-3025	A flaw has been found in ShuoRen Smart Heating Integrated Management Platform 1.0.0. Affected by this vulnerability is an unknown functionality of the file /MP/Service/Webservice/ExampleNodeService.asmx. Executing a manipulation of the argument File can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-3026	A vulnerability has been found in erzhongxmu JEEWMS 3.7. Affected by this issue is some unknown functionality of the file /plug-in/ueditor/jsp/getRemoteImage.jsp of the component UEditor. The manipulation of the argument upfile leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2944	A security flaw has been discovered in Tosei Online Store Management System ネット店舗管理システム 1.01. Affected is the function system of the file /cgi-bin/monitor.php of the component HTTP POST Request Handler. Performing a manipulation of the argument DevId results in os command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-68043	Missing Authorization vulnerability in LottieFiles LottieFiles lottiefiles allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LottieFiles: from n/a through <= 3.0.0.	7.3	More Details
CVE-2026-25926	Notepad++ is a free and open-source source code editor. An Unsafe Search Path vulnerability (CWE-426) exists in versions prior to 8.9.2 when launching Windows Explorer without an absolute executable path. This may allow execution of a malicious explorer.exe if an attacker can control the process working directory. Under certain conditions, this could lead to arbitrary code execution in the context of the running application. Version 8.9.2 patches the issue.	7.3	More Details
CVE-2026-2865	A vulnerability was found in itsourcecode Agri-Trading Online Shopping System 1.0. This impacts an unknown function of the file admin/productcontroller.php of the component HTTP POST Request Handler. Performing a manipulation of the argument Product results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2684	A vulnerability was determined in Tsinghua Unigroup Electronic Archives System up to 3.2.210802(62532). The impacted element is an unknown function of the file /Archive/ErecordManage/uploadFile.html. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2668	A vulnerability was found in Rongzhitong Visual Integrated Command and Dispatch Platform up to 20260206. This affects an unknown function of the file /dm/dispatch/user/add of the component User Handler. The manipulation results in improper access controls. The attack may be launched 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-2026-3053	A vulnerability was determined in DataLinkDC dinky up to 1.2.5. This affects the function addInterceptors of the file dinky-admin/src/main/java/org/dinky/configure/AppConfig.java of the component OpenAPI Endpoint. Executing a manipulation can lead to missing authentication. It is possible to launch 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.	7.3	More Details
CVE-2026-3068	A weakness has been identified in itsourcecode Document Management System 1.0. This impacts an unknown function of the file /deluser.php. Executing a manipulation of the argument user2del can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2025-33181	NVIDIA Cumulus Linux and NVOS products contain a vulnerability in the NVUE interface, where a low-privileged user could inject a command. A successful exploit of this vulnerability might lead to escalation of privileges.	7.3	More Details
CVE-2026-	A vulnerability was detected in itsourcecode Event Management System 1.0. Affected is an unknown function of the file /admin/manage_booking.php. The manipulation of the argument ID results in sql injection. The attack may be performed from	7.3	More

2689	remote. The exploit is now public and may be used.		Details
CVE-2026-2690	A flaw has been found in itsourcecode Event Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login of the component Admin Login. This manipulation of the argument Username 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-2026-26193	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.6.44, aanually modifying chat history allows setting the `embeds` property on a response message, the content of which is loaded into an iFrame with a sandbox that has `allow-scripts` and `allow-same-origin` set, ignoring the "iframe Sandbox Allow Same Origin" configuration. This enables stored XSS on the affected chat. This also triggers when the chat is in the shared format. The result is a shareable link containing the payload that can be distributed to any other users on the instance. Version 0.6.44 fixes the issue.	7.3	More Details
CVE-2026-3069	A security vulnerability has been detected in itsourcecode Document Management System 1.0. Affected is an unknown function of the file /edtlbls.php. The manipulation of the argument field1 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-2848	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=register of the component Registration. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-2691	A vulnerability has been found in itsourcecode Event Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/manage_register.php. Such manipulation of the argument ID 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-2026-26192	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.7.0, aanually modifying chat history allows setting the `html` property within document metadata. This causes the frontend to enter a code path that treats document contents as HTML, and render them in an iFrame when the citation is previewed. This allows stored XSS via a weaponized document payload in a chat. The payload also executes when the citation is viewed on a shared chat. Version 0.7.0 fixes the issue.	7.3	More Details
CVE-2019-25405	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the newLicense parameter. Attackers can send POST requests to the license activation endpoint with script payloads in the newLicense field to execute arbitrary JavaScript in administrators' browsers.	7.2	More Details
CVE-2025-12975	The CTX Feed – WooCommerce Product Feed Manager plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the woo_feed_plugin_installing() function in all versions up to, and including, 6.6.11. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to install arbitrary plugins which can be leveraged to achieve remote code execution.	7.2	More Details
CVE-2026-2847	A vulnerability was detected in UTT HiPER 520 1.7.7-160105. Affected is the function sub_44EFB4 of the file /goform/formReleaseConnect of the component Web Management Interface. The manipulation of the argument Isp_Name results in os command injection. The attack can be launched remotely. The exploit is now public and may be used.	7.2	More Details
CVE-2026-2935	A weakness has been identified in UTT HiPER 810G up to 1.7.7-171114. This issue affects the function strcpy of the file /goform/ConfigExceptMSN. Executing a manipulation of the argument remark can lead to buffer overflow. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-2026-2846	A security vulnerability has been detected in UTT HiPER 520 1.7.7-160105. This impacts the function sub_44D264 of the file /goform/formPdbUpConfig of the component Web Management Interface. The manipulation of the argument policyNames leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.2	More Details
CVE-2025-14905	A flaw was found in the 389-ds-base server. A heap buffer overflow vulnerability exists in the `schema_attr_enum_callback` function within the `schema.c` file. This occurs because the code incorrectly calculates the buffer size by summing alias string lengths without accounting for additional formatting characters. When a large number of aliases are processed, this oversight can lead to a heap overflow, potentially allowing a remote attacker to cause a Denial of Service (DoS) or achieve Remote Code Execution (RCE).	7.2	More Details
CVE-2025-15041	The BackWPup – WordPress Backup & Restore Plugin plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the save_site_option() function in all versions up to, and including, 5.6.2. This makes it possible for authenticated attackers, with level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	7.2	More Details
CVE-2026-2980	A vulnerability has been found in UTT HiPER 810G up to 1.7.7-1711. Impacted is the function strcpy of the file /goform/setSysAdm. The manipulation of the argument passwd1 leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.2	More Details
CVE-2025-14452	The WP Customer Reviews plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wpcr3_fname' parameter in all versions up to, and including, 3.7.5 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.	7.2	More Details
CVE-2026-22766	Dell Wyse Management Suite, versions prior to WMS 5.5, contain an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.	7.2	More Details
CVE-2026-1931	The Rent Fetch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'keyword' parameter in all versions up to, and including, 0.32.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details

CVE-2019-25454	phpMoAdmin 1.1.5 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the collection parameter. Attackers can send GET requests to moadmin.php with script payloads in the collection parameter during collection creation to execute arbitrary JavaScript in users' browsers.	7.2	More Details
CVE-2019-25422	Comodo Dome Firewall 2.7.0 contains cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through the vpnfw endpoint. Attackers can submit POST requests with script payloads in the target parameter for reflected XSS or the remark parameter for stored XSS to execute arbitrary JavaScript in administrator browsers.	7.2	More Details
CVE-2026-25316	Deserialization of Untrusted Data vulnerability in Brainstorm Force CartFlows cartflows allows Object Injection.This issue affects CartFlows: from n/a through <= 2.1.19.	7.2	More Details
CVE-2026-2296	The Product Addons for Woocommerce – Product Options with Custom Fields plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 3.1.0. This is due to insufficient input validation of the 'operator' field in conditional logic rules within the evalConditions() function, which passes unsanitized user input directly to PHP's eval() function. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to inject and execute arbitrary PHP code on the server via the conditional logic 'operator' parameter when saving addon form field rules.	7.2	More Details
CVE-2026-22333	Deserialization of Untrusted Data vulnerability in YITHEMES YITH WooCommerce Compare yith-woocommerce-compare allows Object Injection.This issue affects YITH WooCommerce Compare: from n/a through <= 3.6.0.	7.2	More Details
CVE-2026-2019	The Cart All In One For WooCommerce plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.1.21. This is due to insufficient input validation on the 'Assign page' field which is passed directly to the eval() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute arbitrary PHP code on the server.	7.2	More Details
CVE-2026-26046	A vulnerability was found in a Moodle TeX filter administrative setting where insufficient sanitization of configuration input could allow command injection. On sites where the TeX filter is enabled and ImageMagick is installed, a maliciously crafted setting value entered by an administrator could result in unintended system command execution. While exploitation requires administrative privileges, successful compromise could affect the entire Moodle server.	7.2	More Details
CVE-2026-26045	A flaw was identified in Moodle’s backup restore functionality where specially crafted backup files were not properly validated during processing. If a malicious backup file is restored, it could lead to unintended execution of server-side code. Since restore capabilities are typically available to privileged users, exploitation requires authenticated access. Successful exploitation could result in full compromise of the Moodle server.	7.2	More Details
CVE-2026-26325	OpenClaw is a personal AI assistant. Prior to version 2026.2.14, a mismatch between `rawCommand` and `command[]` in the node host `system.run` handler could cause allowlist/approval evaluation to be performed on one command while executing a different argv. This only impacts deployments that use the node host / companion node execution path (`system.run` on a node), enable allowlist-based exec policy (`security=allowlist`) with approval prompting driven by allowlist misses (for example `ask=on-miss`), allow an attacker to invoke `system.run`. Default/non-node configurations are not affected. Version 2026.2.14 enforces `rawCommand`/`command[]` consistency (gateway fail-fast + node host validation).	7.2	More Details
CVE-2026-1459	A post-authentication command injection vulnerability in the TR-369 certificate download CGI program of the Zyxel VMG3625-T50B firmware versions through 5.50(ABPM.9.7)C0 could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on an affected device.	7.2	More Details
CVE-2026-27177	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability via the /objects/?op=set endpoint, which is intentionally unauthenticated for IoT device integration. User-supplied property values are stored raw in the database without sanitization. When an administrator views the property editor in the admin panel, the stored values are rendered without escaping in both a paragraph tag (SOURCE field) and a textarea element (VALUE field). The XSS fires on page load without requiring any click from the admin. Additionally, the session cookie lacks the HttpOnly flag, enabling session hijack via document.cookie exfiltration. An attacker can enumerate properties via the unauthenticated /api.php/data/ endpoint and poison any property with malicious JavaScript.	7.2	More Details
CVE-2019-25419	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the schedule endpoint. Attackers can submit POST requests with JavaScript payloads in the SCHNAME parameter to execute arbitrary code in administrators' browsers when the schedule page is accessed.	7.2	More Details
CVE-2026-27466	BigBlueButton is an open-source virtual classroom. In versions 3.0.21 and below, the official documentation for "Server Customization" on Support for ClamAV as presentation file scanner contains instructions that leave a BBB server vulnerable for Denial of Service. The flawed command exposes both ports (3310 and 7357) to the internet. A remote attacker can use this to send complex or large documents to clamd and waste server resources, or shutdown the clamd process. The clamd documentation explicitly warns about exposing this port. Enabling ufw (ubuntu firewall) during install does not help, because Docker routes container traffic through the nat table, which is not managed or restricted by ufw. Rules installed by ufw in the filter table have no effect on docker traffic. In addition, the provided example also mounts /var/bigbluebutton with write permissions into the container, which should not be required. Future vulnerabilities in clamd may allow attackers to manipulate files in that folder. Users are unaffected unless they have opted in to follow the extra instructions from BigBlueButton's documentation. This issue has been fixed in version 3.0.22.	7.2	More Details
CVE-2025-69299	Server-Side Request Forgery (SSRF) vulnerability in Laborator Oxygen oxygen allows Server Side Request Forgery.This issue affects Oxygen: from n/a through <= 6.0.8.	7.2	More Details
CVE-2026-2670	A vulnerability was identified in Advantech WISE-6610 1.2.1_20251110. Affected is an unknown function of the file /cgi-bin/luci/admin/openvpn_apply of the component Background Management. Such manipulation of the argument delete_file leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability through method parameter injection into the shoutbox. The /objects/?method= endpoint allows unauthenticated execution of stored methods with attacker-		

CVE-2026-27178	controlled parameters. Default methods such as ThisComputer.VolumeLevelChanged pass the user-supplied VALUE parameter directly into the say() function, which stores the message raw in the shouts database table without escaping. The shoutbox widget renders stored messages without sanitization in both PHP rendering code and HTML templates. Because the dashboard widget auto-refreshes every 3 seconds, the injected script executes automatically when any administrator loads the dashboard, enabling session hijack through cookie exfiltration.	7.2	More Details
CVE-2025-67984	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in calliko NPS computy nps-computy allows DOM-Based XSS.This issue affects NPS computy: from n/a through <= 2.8.2.	7.1	More Details
CVE-2025-67991	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vanquish User Extra Fields wp-user-extra-fields allows Reflected XSS.This issue affects User Extra Fields: from n/a through <= 16.8.	7.1	More Details
CVE-2026-22048	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9.0.12 and 12.0.0.4 with Single Sign-on enabled and configured to use Microsoft Entra ID (formerly Azure AD) as an IdP are susceptible to a Server-Side Request Forgery (SSRF) vulnerability. Successful exploit could allow an authenticated attacker with low privileges to delete configuration data or deny access to some resources.	7.1	More Details
CVE-2025-68031	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in faraz sms افزونه پیامک حرفه ای فراز اس ام اس farazsms allows Reflected XSS.This issue affects افزونه پیامک حرفه ای فراز اس ام اس from n/a through <= 2.7.3.	7.1	More Details
CVE-2025-53228	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jezza101 bbpress Simple Advert Units bbpress-simple-advert-units allows Reflected XSS.This issue affects bbpress Simple Advert Units: from n/a through <= 0.41.	7.1	More Details
CVE-2025-68930	Versions of the Traccar open-source GPS tracking system up to and including 6.11.1 contain a Cross-Site WebSocket Hijacking (CSWSH) vulnerability in the `/api/socket` endpoint. The application fails to validate the `Origin` header during the WebSocket handshake. This allows a remote attacker to bypass the Same Origin Policy (SOP) and establish a full-duplex WebSocket connection using a legitimate user's credentials (JSESSIONID). As of time of publication, it is unclear whether a fix is available.	7.1	More Details
CVE-2025-67971	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPManageNinja FluentCart fluent-cart allows Reflected XSS.This issue affects FluentCart: from n/a through < 1.3.0.	7.1	More Details
CVE-2025-67972	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fox-themes Prague prague-plugins allows Reflected XSS.This issue affects Prague: from n/a through <= 2.2.8.	7.1	More Details
CVE-2026-26960	node-tar is a full-featured Tar for Node.js. When using default options in versions 7.5.7 and below, an attacker-controlled archive can create a hardlink inside the extraction directory that points to a file outside the extraction root, enabling arbitrary file read and write as the extracting user. Severity is high because the primitive bypasses path protections and turns archive extraction into a direct filesystem access primitive. This issue has been fixed in version 7.5.8.	7.1	More Details
CVE-2025-53231	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevstudio Easy Taxonomy Images easy-taxonomy-images allows Stored XSS.This issue affects Easy Taxonomy Images: from n/a through <= 1.0.1.	7.1	More Details
CVE-2025-53233	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RylanH Storyform storyform allows Reflected XSS.This issue affects Storyform: from n/a through <= 0.6.14.	7.1	More Details
CVE-2025-53237	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soflyy WP Wizard Cloak wp-wizard-cloak allows Reflected XSS.This issue affects WP Wizard Cloak: from n/a through <= 1.0.1.	7.1	More Details
CVE-2026-26317	OpenClaw is a personal AI assistant. Prior to 2026.2.14, browser-facing localhost mutation routes accepted cross-origin browser requests without explicit Origin/Referer validation. Loopback binding reduces remote exposure but does not prevent browser-initiated requests from malicious origins. A malicious website can trigger unauthorized state changes against a victim's local OpenClaw browser control plane (for example opening tabs, starting/stopping the browser, mutating storage/cookies) if the browser control service is reachable on loopback in the victim's browser context. Starting in version 2026.2.14, mutating HTTP methods (POST/PUT/PATCH/DELETE) are rejected when the request indicates a non-loopback Origin/Referer (or `Sec-Fetch-Site: cross-site`). Other mitigations include enabling browser control auth (token/password) and avoid running with auth disabled.	7.1	More Details
CVE-2025-67978	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FixBD Educare educare allows Reflected XSS.This issue affects Educare: from n/a through <= 1.6.1.	7.1	More Details
CVE-2026-24948	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fox-themes Reflector reflector-plugins allows Reflected XSS.This issue affects Reflector: from n/a through <= 1.2.2.	7.1	More Details
CVE-2025-68037	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Atlas Gondal Export Media URLs export-media-urls allows Reflected XSS.This issue affects Export Media URLs: from n/a through <= 2.2.	7.1	More Details
CVE-2025-68856	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in keeswolters Mopinion Feedback Form mopinion-feedback-form allows DOM-Based XSS.This issue affects Mopinion Feedback Form: from n/a through <= 1.1.1.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in peterwsterling Simple		More

2025-68880	Archive Generator simple-archive-generator allows Reflected XSS.This issue affects Simple Archive Generator: from n/a through <= 5.2.	7.1	Details
CVE-2025-69296	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhostPool Aardvark aardvark allows Reflected XSS.This issue affects Aardvark: from n/a through <= 4.6.3.	7.1	More Details
CVE-2025-69302	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes DesignThemes Core Features designthemes-core-features allows Reflected XSS.This issue affects DesignThemes Core Features: from n/a through <= 2.3.	7.1	More Details
CVE-2025-69323	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs Slimstat Analytics wp-slimstat allows Reflected XSS.This issue affects Slimstat Analytics: from n/a through <= 5.3.2.	7.1	More Details
CVE-2025-69324	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms nex-forms-express-wp-form-builder allows Stored XSS.This issue affects NEX-Forms: from n/a through <= 9.1.7.	7.1	More Details
CVE-2025-69326	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 <= 9.1.7.	7.1	More Details
CVE-2025-69330	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jthemes Prestige prestige allows Reflected XSS.This issue affects Prestige: from n/a through < 1.4.1.	7.1	More Details
CVE-2025-69367	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3themes Oyster - Photography WordPress Theme oyster allows DOM-Based XSS.This issue affects Oyster - Photography WordPress Theme: from n/a through <= 4.4.3.	7.1	More Details
CVE-2025-69368	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3themes SOHO - Photography WordPress Theme soho allows DOM-Based XSS.This issue affects SOHO - Photography WordPress Theme: from n/a through <= 3.0.3.	7.1	More Details
CVE-2025-69384	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdiscover Timeline Event History timeline-event-history allows Reflected XSS.This issue affects Timeline Event History: from n/a through <= 3.2.	7.1	More Details
CVE-2025-69386	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realvirtualmx RVCFDI para Woocommerce rvcfdi-para-woocommerce allows Reflected XSS.This issue affects RVCFDI para Woocommerce: from n/a through <= 8.1.8.	7.1	More Details
CVE-2025-69389	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hugh Mungus Visitor Maps Extended Referer Field visitor-maps-extended-referer-field allows Reflected XSS.This issue affects Visitor Maps Extended Referer Field: from n/a through <= 1.2.6.	7.1	More Details
CVE-2025-69390	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themebon Business Template Blocks for WPBakery (Visual Composer) Page Builder templates-and-addons-for-wpbakery-page-builder allows Reflected XSS.This issue affects Business Template Blocks for WPBakery (Visual Composer) Page Builder: from n/a through <= 1.3.2.	7.1	More Details
CVE-2025-69391	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3themes Diamond diamond allows Reflected XSS.This issue affects Diamond: from n/a through <= 2.4.8.	7.1	More Details
CVE-2025-69392	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in itex iMoney imoney allows Reflected XSS.This issue affects iMoney: from n/a through <= 0.36.	7.1	More Details
CVE-2026-23547	Missing Authorization vulnerability in cmsmasters CMSMasters Content Composer cmsmasters-content-composer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CMSMasters Content Composer: from n/a through <= 2.5.8.	7.1	More Details
CVE-2026-22352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PersianScript Persian Woocommerce SMS persian-woocommerce-sms allows Reflected XSS.This issue affects Persian Woocommerce SMS: from n/a through <= 7.1.1.	7.1	More Details
CVE-2026-22357	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spencer Haws Link Whisper Free link-whisper allows Reflected XSS.This issue affects Link Whisper Free: from n/a through <= 0.9.0.	7.1	More Details
CVE-2026-27170	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. In versions 1.1.2-alpha and below, URL ingest allows overly permissive server-side fetch behavior and can be coerced into requesting unsafe targets. Potential access/probing of private/local network resources from the OpenSift host process when ingesting attacker-controlled URLs. This issue has been fixed in version 1.1.3-alpha. To workaround when using trusted local-only exceptions, use OPENSIFT_ALLOW_PRIVATE_URLS=true with caution.	7.1	More Details
CVE-2026-	ADB Explorer is a fluent UI for ADB on Windows. Versions 0.9.26020 and below have an unvalidated command-line argument that allows any user to trigger recursive deletion of arbitrary directories on the Windows filesystem. ADB Explorer accepts an optional path argument to set a custom data directory, but only check whether the path exists. The ClearDrag() method calls Directory.Delete(dir, true) on every subdirectory of that path at both application startup and exit. An attacker can craft a malicious shortcut (.lnk) or batch script that launches ADB Explorer with a critical directory (e.g.	7.1	More Details

27115	C:\Users\%USERNAME%\Documents) as the argument, causing permanent recursive deletion of all its subdirectories. Any user who launches ADB Explorer via a crafted shortcut, batch file, or script loses the contents of the targeted directory permanently (deletion bypasses the Recycle Bin). This issue has been fixed in version 0.9.26021.		
CVE-2026-26721	An issue in Key Systems Inc Global Facilities Management Software v.20230721a allows a remote attacker to obtain sensitive information via the sid query parameter.	7.1	More Details
CVE-2026-27072	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PixelYourSite PixelYourSite – Your smart PIXEL (TAG) Manager pixelyoursite allows Stored XSS.This issue affects PixelYourSite – Your smart PIXEL (TAG) Manager: from n/a through <= 11.2.0.1.	7.1	More Details
CVE-2026-24955	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fox-themes Whizz Plugins whizz-plugins allows Reflected XSS.This issue affects Whizz Plugins: from n/a through <= 1.9.	7.1	More Details
CVE-2026-24949	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods PhotoMe photome allows DOM-Based XSS.This issue affects PhotoMe: from n/a through <= 5.7.1.	7.1	More Details
CVE-2026-24943	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Conference grandconference allows Reflected XSS.This issue affects Grand Conference: from n/a through <= 5.3.4.	7.1	More Details
CVE-2025-68863	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zack Katz iContact for Gravity Forms gravity-forms-icontact allows Reflected XSS.This issue affects iContact for Gravity Forms: from n/a through <= 1.3.2.	7.1	More Details
CVE-2025-67990	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 GMap Targeting gmap-targeting allows Reflected XSS.This issue affects GMap Targeting: from n/a through <= 1.1.7.	7.1	More Details
CVE-2025-68854	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in harman79 ID Arrays id-arrays allows DOM-Based XSS.This issue affects ID Arrays: from n/a through <= 2.1.2.	7.1	More Details
CVE-2025-68845	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aThemeArt Translations eDS Responsive Menu eds-responsive-menu allows Reflected XSS.This issue affects eDS Responsive Menu: from n/a through <= 1.2.	7.1	More Details
CVE-2025-68069	Missing Authorization vulnerability in wpWax Directorist directorist allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Directorist: from n/a through <= 8.5.10.	7.1	More Details
CVE-2025-68495	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine jet-engine allows Reflected XSS.This issue affects JetEngine: from n/a through <= 3.8.0.	7.1	More Details
CVE-2025-68501	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mollie Mollie Payments for WooCommerce mollie-payments-for-woocommerce allows Reflected XSS.This issue affects Mollie Payments for WooCommerce: from n/a through <= 8.1.1.	7.1	More Details
CVE-2025-68852	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webmuehle Court Reservation court-reservation allows Reflected XSS.This issue affects Court Reservation: from n/a through <= 1.10.9.	7.1	More Details
CVE-2025-68842	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in totalbounty Widget Logic Visual widget-logic-visual allows Reflected XSS.This issue affects Widget Logic Visual: from n/a through <= 1.52.	7.1	More Details
CVE-2025-68843	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bas Schuiling FeedWordPress Advanced Filters faf allows Reflected XSS.This issue affects FeedWordPress Advanced Filters: from n/a through <= 0.6.2.	7.1	More Details
CVE-2025-68844	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DaleAB Membee Login membees-member-login-widget allows Reflected XSS.This issue affects Membee Login: from n/a through <= 2.3.6.	7.1	More Details
CVE-2019-25450	Dolibarr ERP/CRM 10.0.1 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries by injecting SQL code through POST parameters. Attackers can inject malicious SQL through parameters like actioncode, demand_reason_id, and availability_id in card.php endpoints to extract sensitive database information using boolean-based blind, error-based, and time-based blind techniques.	7.1	More Details
CVE-2025-68846	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paris Holley Asynchronous Javascript asynchronous-javascript allows Reflected XSS.This issue affects Asynchronous Javascript: from n/a through <= 1.3.5.	7.1	More Details
CVE-2025-68848	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in anmari amr cron manager amr-cron-manager allows Reflected XSS.This issue affects amr cron manager: from n/a through <= 2.3.	7.1	More Details
CVE-			

2025-68847	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in itex iSape isape allows Reflected XSS.This issue affects iSape: from n/a through <= 0.72.	7.1	More Details
CVE-2026-20138	In Splunk Enterprise versions below 10.2.0, 10.0.2, 9.4.7, 9.3.9, and 9.2.11, a user of a Splunk Search Head Cluster (SHC) deployment who holds a role with access to the Splunk `_internal` index could view the `integrationKey`, `secretKey`, and `appSecretKey` secrets, generated by [Duo Two-Factor Authentication for Splunk Enterprise](https://duo.com/docs/splunk), in plain text.	6.8	More Details
CVE-2026-20142	In Splunk Enterprise versions below 10.2.0, 10.0.2, 9.4.7, 9.3.9, and 9.2.11, a user of a Splunk Search Head Cluster (SHC) deployment who holds a role with access to the Splunk `_internal` index could view the RSA `accessKey` value from the [<u>Authentication.conf</u>](https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.2/configuration-file-reference/10.2.0-configuration-file-reference/authentication.conf)file, in plain text.	6.8	More Details
CVE-2026-27125	svelte performance oriented web framework. Prior to 5.51.5, in server-side rendering, attribute spreading on elements (e.g. <div {...attrs}>) enumerates inherited properties from the object's prototype chain rather than only own properties. In environments where Object.prototype has already been polluted — a precondition outside of Svelte's control — this can cause unexpected attributes to appear in SSR output or cause SSR to throw errors. Client-side rendering is not affected. This vulnerability is fixed in 5.51.5.	6.8	More Details
CVE-2026-20144	In Splunk Enterprise versions below 10.2.0, 10.0.2, 9.4.7, 9.3.8, and 9.2.11, and Splunk Cloud Platform versions below 10.2.2510.0, 10.1.2507.11, 10.0.2503.9, and 9.3.2411.120, a user of a Splunk Search Head Cluster (SHC) deployment who holds a role with access to the the Splunk _internal index could view the Security Assertion Markup Language (SAML) configurations for Attribute query requests (AQRs) or Authentication extensions in plain text within the conf.log file, depending on which feature is configured.	6.8	More Details
CVE-2025-10010	The CPSD CryptoPro Secure Disk application boots a small Linux operating system to perform user authentication before using BitLocker to decrypt the Windows partition. The system is located on a separate unencrypted partition which can be reached by anyone with access to the hard disk. Multiple checks are performed to validate the integrity of the Linux operating system and the CryptoPro Secure Disk application files. When files are changed an error is shown on system start. One of the checks is the Linux kernel's Integrity Measurement Architecture (IMA). It was identified that configuration files are not validated by the IMA and can then (if not checked by other measures) be changed. This allows an attacker to execute arbitrary code in the context of the root user and enables an attacker to e.g., plant a backdoor and access data during execution.	6.8	More Details
CVE-2026-26972	OpenClaw is a personal AI assistant. In versions 2026.1.12 through 2026.2.12, OpenClaw browser download helpers accepted an unsanitized output path. When invoked via the browser control gateway routes, this allowed path traversal to write downloads outside the intended OpenClaw temp downloads directory. This issue is not exposed via the AI agent tool schema (no `download` action). Exploitation requires authenticated CLI access or an authenticated gateway RPC token. Version 2026.2.13 fixes the issue.	6.7	More Details
CVE-2026-27008	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a bug in `download` skill installation allowed `targetDir` values from skill frontmatter to resolve outside the per-skill tools directory if not strictly validated. In the admin-only `skills.install` flow, this could write files outside the intended install sandbox. Version 2026.2.15 contains a fix for the issue.	6.7	More Details
CVE-2026-3091	An uncontrolled search path element vulnerability in Synology Presto Client before 2.1.3-0672 allows local users to read or write arbitrary files during installation by placing a malicious DLL in advance in the same directory as the installer.	6.7	More Details
CVE-2026-26282	NanaZip is an open source file archive Starting in version 5.0.1252.0 and prior to version 6.0.1630.0, NanaZip has an out-of-bounds heap read in `.NET Single File` bundle header parser due to missing bounds check. Opening a crafted file with NanaZip causes a crash or leaks heap data to the user. Version 6.0.1630.0 patches the issue.	6.6	More Details
CVE-2026-25603	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Linksys MR9600, Linksys MX4200 allows that contents of a USB drive partition can be mounted in an arbitrary location of the file system. This may result in the execution of shell scripts in the context of a root user.This issue affects MR9600: 1.0.4.205530; MX4200: 1.0.13.210200.	6.6	More Details
CVE-2026-24126	Weblate is a web based localization tool. Prior to 5.16.0, the SSH management console did not validate the passed input while adding the SSH host key, which could lead to an argument injection to `ssh-add`. Version 5.16.0 fixes the issue. As a workaround, properly limit access to the management console.	6.6	More Details
CVE-2026-27189	OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Versions 1.1.2-alpha and below, use non-atomic and insufficiently synchronized local JSON persistence flows, potentially causing concurrent operations to lose updates or corrupt local state across sessions/study/quiz/flashcard/wellness/auth stores. This issue has been fixed in version 1.1.3-alpha.	6.6	More Details
CVE-2026-2984	A vulnerability was identified in SourceCodester Student Result Management System 1.0. This affects an unknown function of the file /admin/core/drop_user.php. Such manipulation of the argument ID leads to denial of service. The attack can be executed remotely. The exploit is publicly available and might be used.	6.5	More Details
CVE-2025-27555	Airflow versions before 2.11.1 have a vulnerability that allows authenticated users with audit log access to see sensitive values in audit logs which they should not see. When sensitive connection parameters were set via airflow CLI, values of those variables appeared in the audit log and were stored unencrypted in the Airflow database. While this risk is limited to users with audit log access, it is recommended to upgrade to Airflow 2.11.1 or a later version, which addresses this issue. Users who previously used the CLI to set connections should manually delete entries with those connection sensitive values from the log table. This is similar but not the same issue as CVE-2024-50378	6.5	More Details
CVE-2019-25436	Sricam DeviceViewer 3.12.0.1 contains a password change security bypass vulnerability that allows authenticated users to change passwords without proper validation of the old password field. Attackers can inject a large payload into the old password parameter during the change password process to bypass validation and set an arbitrary new password.	6.5	More Details
CVE-2026-	PJSIP is a free and open source multimedia communication library. Versions prior to 2.17 have a critical heap buffer underflow vulnerability in PJSIP's H.264 packetizer. The bug occurs when processing malformed H.264 bitstreams without NAL unit start	6.5	More

26203	codes, where the packetizer performs unchecked pointer arithmetic that can read from memory located before the allocated buffer. Version 2.17 contains a patch for the issue.		Details
CVE-2025-67624	Missing Authorization vulnerability in Arya Dhiratara Optimize More! – Images optimize-more-images allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Optimize More! – Images: from n/a through <= 1.1.3.	6.5	More Details
CVE-2026-27567	Payload is a free and open source headless content management system. Prior to 3.75.0, a Server-Side Request Forgery (SSRF) vulnerability exists in Payload's external file upload functionality. When processing external URLs for file uploads, insufficient validation of HTTP redirects could allow an authenticated attacker to access internal network resources. The Payload environment must have at least one collection with `upload` enabled and a user who has `create` access to that upload-enabled collection in order to be vulnerable. An authenticated user with upload collection write permissions could potentially access internal services. Response content from internal services could be retrieved through the application. This vulnerability has been patched in v3.75.0. As a workaround, one may mitigate this vulnerability by disabling external file uploads via the `disableExternalFile` upload collection option, or by restricting `create` access on upload-enabled collections to trusted users only.	6.5	More Details
CVE-2026-27022	@langchain/langgraph-checkpoint-redis is the Redis checkpoint and store implementation for LangGraph. A query injection vulnerability exists in the @langchain/langgraph-checkpoint-redis package's filter handling. The RedisSaver and ShallowRedisSaver classes construct RediSearch queries by directly interpolating user-provided filter keys and values without proper escaping. RediSearch has special syntax characters that can modify query behavior, and when user-controlled data contains these characters, the query logic can be manipulated to bypass intended access controls. This vulnerability is fixed in 1.0.2.	6.5	More Details
CVE-2025-59819	This vulnerability allows authenticated attackers to read an arbitrary file by changing a filepath parameter into an internal system path.	6.5	More Details
CVE-2026-26981	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.3.0 through 3.3.6 and 3.4.0 through 3.4.4, a heap-buffer-overflow (OOB read) occurs in the `istream_nonparallel_read` function in `ImfContextInit.cpp` when parsing a malformed EXR file through a memory-mapped `IStream`. A signed integer subtraction produces a negative value that is implicitly converted to `size_t`, resulting in a massive length being passed to `memcpy`. Versions 3.3.7 and 3.4.5 contain a patch.	6.5	More Details
CVE-2026-26057	Skill Scanner is a security scanner for AI Agent Skills that detects prompt injection, data exfiltration, and malicious code patterns. A vulnerability in the API Server of Skill Scanner could allow a unauthenticated, remote attacker to interact with the server API and either trigger a denial of service (DoS) condition or upload arbitrary files. This vulnerability is due to an erroneous binding to multiple interfaces. An attacker could exploit this vulnerability by sending API requests to a device exposing the affected API Server. A successful exploit could allow the attacker to consume an excessive amount of resources (memory starvation) or to upload files to arbitrary folders on the affected device. This vulnerability affects Skill-scanner 1.0.1 and earlier releases when the API Server is enabled. The API Server is not enabled by default. Skill-scanner software releases 1.0.2 and later contain the fix for this vulnerability.	6.5	More Details
CVE-2025-68050	Missing Authorization vulnerability in Leadpages Leadpages leadpages allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Leadpages: from n/a through <= 1.1.3.	6.5	More Details
CVE-2025-67993	Missing Authorization vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Atarim: from n/a through <= 4.2.1.	6.5	More Details
CVE-2026-26338	Hyland Alfresco Transformation Service allows unauthenticated attackers to achieve server-side request forgery (SSRF) through the document processing functionality.	6.5	More Details
CVE-2026-27521	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior do not implement rate limiting or account lockout on failed login attempts, enabling brute-force attacks against user credentials.	6.5	More Details
CVE-2025-68000	Missing Authorization vulnerability in PickPlugins Testimonial Slider testimonial allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Testimonial Slider: from n/a through <= 2.0.15.	6.5	More Details
CVE-2025-68005	Missing Authorization vulnerability in themewant Easy Hotel Booking easy-hotel allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Hotel Booking: from n/a through <= 1.8.7.	6.5	More Details
CVE-2025-68024	Missing Authorization vulnerability in Addonify Addonify – WooCommerce Wishlist addonify-wishlist allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Addonify – WooCommerce Wishlist: from n/a through <= 2.0.15.	6.5	More Details
CVE-2026-26312	Stalwart is a mail and collaboration server. A denial-of-service vulnerability exists in Stalwart Mail Server versions 0.13.0 through 0.15.4 where accessing a specially crafted email containing malformed nested `message/rfc822` MIME parts via IMAP or JMAP causes excessive CPU and memory consumption, potentially leading to an out-of-memory condition and server crash. The malformed structure causes the `mail-parser` crate to produce cyclical references in its parsed representation, which Stalwart then follows indefinitely. Version 0.15.5 contains a patch.	6.5	More Details
CVE-2026-27440	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saad Iqbal myCred mycred allows Stored XSS.This issue affects myCred: from n/a through <= 2.9.7.6.	6.5	More Details
	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and		

CVE-2026-26284	6.9.13-40, ImageMagick lacks proper boundary checking when processing Huffman-coded data from PCD (Photo CD) files. The decoder contains an function that has an incorrect initialization that could cause an out of bounds read. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.5	More Details
CVE-2026-22351	Missing Authorization vulnerability in Marcus (aka @msykes) WP FullCalendar wp-fullcalendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP FullCalendar: from n/a through <= 1.6.	6.5	More Details
CVE-2026-2350	Tanium addressed an insertion of sensitive information into log file vulnerability in Interact and TDS.	6.5	More Details
CVE-2026-21864	Valkey-Bloom is a Rust based Valkey module which brings a Bloom Filter (Module) data type into the Valkey distributed key-value database. Prior to commit a68614b6e3845777d383b3a513cedcc08b3b7ccd, a specially crafted `RESTORE` command can cause Valkey to hit an assertion, causes the server to shutdown. Valkey modules are required to handle errors in RDB parsing by using `VALKEYMODULE_OPTIONS_HANDLE_IO_ERRORS` flag. If this flag is not set, errors encountered during parsing result in a system assertion which shuts down the system. Even though the Valkey-bloom module correctly handled the parsing, it did not originally set the flag. Commit a68614b6e3845777d383b3a513cedcc08b3b7ccd contains a patch. One may mitigate this defect by disabling the `RESTORE` command if it is unused by one's application.	6.5	More Details
CVE-2026-26329	OpenClaw is a personal AI assistant. Prior to version 2026.2.14, authenticated attackers can read arbitrary files from the Gateway host by supplying absolute paths or path traversal sequences to the browser tool's `upload` action. The server passed these paths to Playwright's `setInputFiles()` APIs without restricting them to a safe root. An attacker must reach the Gateway HTTP surface (or otherwise invoke the same browser control hook endpoints); present valid Gateway auth (bearer token / password), as required by the Gateway configuration (In common default setups, the Gateway binds to loopback and the onboarding wizard generates a gateway token even for loopback); and have the `browser` tool permitted by tool policy for the target session/context (and have browser support enabled). If an operator exposes the Gateway beyond loopback (LAN/tailnet/custom bind, reverse proxy, tunnels, etc.), the impact increases accordingly. Starting in version 2026.2.14, the upload paths are now confined to OpenClaw's temp uploads root (`DEFAULT_UPLOAD_DIR`) and traversal/escape paths are rejected.	6.5	More Details
CVE-2026-26328	OpenClaw is a personal AI assistant. Prior to version 2026.2.14, under iMessage `groupPolicy=allowlist`, group authorization could be satisfied by sender identities coming from the DM pairing store, broadening DM trust into group contexts. Version 2026.2.14 fixes the issue.	6.5	More Details
CVE-2025-68026	Missing Authorization vulnerability in Niaj Morshed LC Wizard ghl-wizard allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LC Wizard: from n/a through <= 2.1.1.	6.5	More Details
CVE-2026-2698	An improper access control vulnerability exists where an authenticated user could access areas outside of their authorized scope.	6.5	More Details
CVE-2026-26327	OpenClaw is a personal AI assistant. Discovery beacons (Bonjour/mDNS and DNS-SD) include TXT records such as `lanHost`, `tailnetDns`, `gatewayPort`, and `gatewayTlsSha256`. TXT records are unauthenticated. Prior to version 2026.2.14, some clients treated TXT values as authoritative routing/pinning inputs. iOS and macOS used TXT-provided host hints (`lanHost`/`tailnetDns`) and ports (`gatewayPort`) to build the connection URL. iOS and Android allowed the discovery-provided TLS fingerprint (`gatewayTlsSha256`) to override a previously stored TLS pin. On a shared/untrusted LAN, an attacker could advertise a rogue `_openclaw-gw._tcp` service. This could cause a client to connect to an attacker-controlled endpoint and/or accept an attacker certificate, potentially exfiltrating Gateway credentials (`auth.token` / `auth.password`) during connection. As of time of publication, the iOS and Android apps are alpha/not broadly shipped (no public App Store / Play Store release). Practical impact is primarily limited to developers/testers running those builds, plus any other shipped clients relying on discovery on a shared/untrusted LAN. Version 2026.2.14 fixes the issue. Clients now prefer the resolved service endpoint (SRV + A/AAAA) over TXT-provided routing hints. Discovery-provided fingerprints no longer override stored TLS pins. In iOS/Android, first-time TLS pins require explicit user confirmation (fingerprint shown; no silent TOFU) and discovery-based direct connects are TLS-only. In Android, hostname verification is no longer globally disabled (only bypassed when pinning).	6.5	More Details
CVE-2026-27514	Shenzhen Tenda F3 Wireless Router firmware V12.01.01.55_multi contains a sensitive information exposure vulnerability in the configuration download functionality. The configuration download response includes the router password and administrative password in plaintext. The endpoint also omits appropriate Cache-Control directives, which can allow the response to be stored in client-side caches and recovered by other local users or processes with access to cached browser data.	6.5	More Details
CVE-2025-69385	Missing Authorization vulnerability in AgniHD Cartify - WooCommerce Gutenberg WordPress Theme cartify allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cartify - WooCommerce Gutenberg WordPress Theme: from n/a through <= 1.3.	6.5	More Details
CVE-2026-25897	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, an Integer Overflow vulnerability exists in the sun decoder. On 32-bit systems/builds, a carefully crafted image can lead to an out of bounds heap write. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.5	More Details
CVE-2026-25898	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, the UIL and XPM image encoder do not validate the pixel index value returned by `GetPixelIndex()` before using it as an array subscript. In HDRI builds, `Quantum` is a floating-point type, so pixel index values can be negative. An attacker can craft an image with negative pixel index values to trigger a global buffer overflow read during conversion, leading to information disclosure or a process crash. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.5	More Details
CVE-2026-	uTLS is a fork of crypto/tls, created to customize ClientHello for fingerprinting resistance while still using it for the handshake. In versions 1.6.7 and below, uTLS did not implement the TLS 1.3 downgrade protection mechanism specified in RFC 8446 Section 4.1.3 when using a uTLS ClientHello spec. This allowed an active network adversary to downgrade TLS 1.3 connections initiated by a uTLS client to a lower TLS version (e.g., TLS 1.2) by modifying the ClientHello message to exclude the SupportedVersions	6.5	More

26994	extension, causing the server to respond with a TLS 1.2 ServerHello (along with a downgrade canary in the ServerHello random field). Because uTLS did not check the downgrade canary in the ServerHello random field, clients would accept the downgraded connection without detecting the attack. This attack could also be used by an active network attacker to fingerprint uTLS connections. This issue has been fixed in version 1.7.0.		Details
CVE-2025-69388	Missing Authorization vulnerability in cliengo Cliengo – Chatbot cliengo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cliengo – Chatbot: from n/a through <= 3.0.4.	6.5	More Details
CVE-2025-68542	Missing Authorization vulnerability in vgdevsolutions Checkout Gateway for IRIS checkout-gateway-iris allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Checkout Gateway for IRIS: from n/a through <= 1.3.	6.5	More Details
CVE-2026-26320	OpenClaw is a personal AI assistant. OpenClaw macOS desktop client registers the `openclaw://` URL scheme. For `openclaw://agent` deep links without an unattended `key`, the app shows a confirmation dialog that previously displayed only the first 240 characters of the message, but executed the full message after the user clicked "Run." At the time of writing, the OpenClaw macOS desktop client is still in beta. In versions 2026.2.6 through 2026.2.13, an attacker could pad the message with whitespace to push a malicious payload outside the visible preview, increasing the chance a user approves a different message than the one that is actually executed. If a user runs the deep link, the agent may perform actions that can lead to arbitrary command execution depending on the user's configured tool approvals/allowlists. This is a social-engineering mediated vulnerability: the confirmation prompt could be made to misrepresent the executed message. The issue is fixed in 2026.2.14. Other mitigations include not approve unexpected "Run OpenClaw agent?" prompts triggered while browsing untrusted sites and usingunattended deep links only with a valid `key` for trusted personal automations.	6.5	More Details
CVE-2026-25982	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap out-of-bounds read vulnerability exists in the `coders/dcm.c` module. When processing DICOM files with a specific configuration, the decoder loop incorrectly reads bytes per iteration. This causes the function to read past the end of the allocated buffer, potentially leading to a Denial of Service (crash) or Information Disclosure (leaking heap memory into the image). Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.5	More Details
CVE-2025-70044	An issue pertaining to CWE-295: Improper Certificate Validation was discovered in fofolee uTools-quickcommand 5.0.3.	6.5	More Details
CVE-2026-24944	Missing Authorization vulnerability in weDevs Subscribe2 subscribe2 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Subscribe2: from n/a through <= 10.44.	6.5	More Details
CVE-2026-23521	Versions of the Traccar open-source GPS tracking system up to and including 6.11.1 contain an issue in which authenticated users who can create or edit devices can set a device `uniqueId` to an absolute path. When uploading a device image, Traccar uses that `uniqueId` to build the filesystem path without enforcing that the resolved path stays under the media root. This allows writing files outside the media directory. As of time of publication, it is unclear whether a fix is available.	6.5	More Details
CVE-2025-14339	The weMail - Email Marketing, Lead Generation, Optin Forms, Email Newsletters, A/B Testing, and Automation plugin for WordPress is vulnerable to unauthorized form deletion in all versions up to, and including, 2.0.7. This is due to the `Forms::permission()` callback only validating the `X-WP-Nonce` header without checking user capabilities. Since the REST nonce is exposed to unauthenticated visitors via the `weMail` JavaScript object on pages with weMail forms, any unauthenticated user can permanently delete all weMail forms by extracting the nonce from the page source and sending a DELETE request to the forms endpoint.	6.5	More Details
CVE-2025-68534	Missing Authorization vulnerability in add-ons.org PDF for WPForms pdf-for-wpforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PDF for WPForms: from n/a through <= 6.3.0.	6.5	More Details
CVE-2026-26047	A denial-of-service vulnerability was identified in Moodle’s TeX formula editor. When rendering TeX content using mimetex, insufficient execution time limits could allow specially crafted formulas to consume excessive server resources. An authenticated user could abuse this behavior to degrade performance or cause service interruption.	6.5	More Details
CVE-2025-65995	When a DAG failed during parsing, Airflow’s error-reporting in the UI could include the full kwargs passed to the operators. If those kwargs contained sensitive values (such as secrets), they might be exposed in the UI tracebacks to authenticated users who had permission to view that DAG. The issue has been fixed in Airflow 3.1.4 and 2.11.1, and users are strongly advised to upgrade to prevent potential disclosure of sensitive information.	6.5	More Details
CVE-2026-1292	Tanium addressed an insertion of sensitive information into log file vulnerability in Trends.	6.5	More Details
CVE-2026-1344	Tanium addressed an insecure file permissions vulnerability in Enforce Recovery Key Portal.	6.5	More Details
CVE-2026-25372	Missing Authorization vulnerability in Kodezen LLC Academy LMS academy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Academy LMS: from n/a through <= 3.5.3.	6.5	More Details
CVE-2025-11725	The Aruba HiSpeed Cache plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability checks on the multiple functions in all versions up to, and including, 3.0.2. This makes it possible for unauthenticated attackers to modify plugin's configuration settings, enable or disable features, as well as enable/disable WordPress cron jobs or debug mode	6.5	More Details
	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 7.37. This is due to insufficient escaping on the `file_name` parameter which is stored in the database during		

CVE-2026-1317	file upload and later used in raw SQL queries without proper sanitization. This makes it possible for authenticated attackers with Subscriber-level access or higher to append additional SQL queries into already existing queries via a malicious filename, which can be used to extract sensitive information from the database. The vulnerability can only be exploited when the 'Single Import/Export' option is enabled, and the server is running a PHP version < 8.0.	6.5	More Details
CVE-2026-1639	The Taskbuilder – WordPress Project Management & Task Management plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'order' and 'sort_by' parameters in all versions up to, and including, 5.0.2 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.	6.5	More Details
CVE-2026-2669	A vulnerability was determined in Rongzhitong Visual Integrated Command and Dispatch Platform up to 20260206. This impacts an unknown function of the file /dm/dispatch/user/delete of the component User Handler. This manipulation of the argument ID causes improper access controls. Remote exploitation of the attack is possible. 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.	6.5	More Details
CVE-2026-25368	Missing Authorization vulnerability in codepeople Calculated Fields Form calculated-fields-form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Calculated Fields Form: from n/a through <= 5.4.4.1.	6.5	More Details
CVE-2026-1999	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed an attacker to merge their own pull request into a repository without having push access by exploiting an authorization bypass in the enable_auto_merge mutation for pull requests. This issue only affected repositories that allow forking as the attack relies on opening a pull request from an attacker-controlled fork into the target repository. Exploitation was only possible in specific scenarios. It required a clean pull request status and only applied to branches without branch protection rules enabled. This vulnerability affected GitHub Enterprise Server versions prior to 3.19.2, 3.18.5, and 3.17.11, and was fixed in versions 3.19.2, 3.18.5, and 3.17.11. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2026-1355	A Missing Authorization vulnerability was identified in GitHub Enterprise Server that allowed an attacker to upload unauthorized content to another user’s repository migration export due to a missing authorization check in the repository migration upload endpoint. By supplying the migration identifier, an attacker could overwrite or replace a victim’s migration archive, potentially causing victims to download attacker-controlled repository data during migration restores or automated imports. An attacker would require authentication to the victim's GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.20 and was fixed in versions 3.19.2, 3.18.5, 3.17.11, 3.16.14, 3.15.18, 3.14.23. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2026-0665	An off-by-one error was found in QEMU's KVM Xen guest support. A malicious guest could use this flaw to trigger out-of-bounds heap accesses in the QEMU process via the emulated Xen physdev hypercall interface, leading to a denial of service or potential memory corruption.	6.5	More Details
CVE-2025-70063	The 'Medical History' module in PHPGurukul Hospital Management System v4.0 contains an Insecure Direct Object Reference (IDOR) vulnerability. The application fails to verify that the requested 'viewid' parameter belongs to the currently authenticated patient. This allows a user to access the confidential medical records of other patients by iterating the 'viewid' integer.	6.5	More Details
CVE-2026-25432	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in omnipressteam Omnipress omnipress allows Stored XSS.This issue affects Omnipress: from n/a through <= 1.6.7.	6.5	More Details
CVE-2025-70062	PHPGurukul Hospital Management System v4.0 contains a Cross-Site Request Forgery (CSRF) vulnerability in the 'Add Doctor' module. The application fails to enforce CSRF token validation on the add-doctor.php endpoint. This allows remote attackers to create arbitrary Doctor accounts (privileged users) by tricking an authenticated administrator into visiting a malicious page.	6.5	More Details
CVE-2026-25451	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Page Builder bold-page-builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through <= 5.6.4.	6.5	More Details
CVE-2026-25453	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mdempfle Advanced iFrame advanced-iframe allows DOM-Based XSS.This issue affects Advanced iFrame: from n/a through <= 2025.10.	6.5	More Details
CVE-2026-25463	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WpEstate Wpresidence Core wpresidence-core allows Stored XSS.This issue affects Wpresidence Core: from n/a through <= 5.4.0.	6.5	More Details
CVE-2026-25472	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Fusion Builder fusion-builder allows Stored XSS.This issue affects Fusion Builder: from n/a through <= 3.14.3.	6.5	More Details
CVE-2026-26361	Dell Unisphere for PowerMax, version(s) 10.2, contain(s) an External Control of File Name or Path vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	6.5	More Details
CVE-2025-65519	mayswind ezbookkeeping versions 1.2.0 and earlier contain a critical vulnerability in JSON and XML file import processing. The application fails to validate nesting depth during parsing operations, allowing authenticated attackers to trigger denial of service conditions by uploading deeply nested malicious files. This results in CPU exhaustion, service degradation, or complete service unavailability.	6.5	More Details
CVE-2026-1436	Improper Access Control (IDOR) in the Graylog API, version 2.2.3, which occurs when modifying the user ID in the URL. An authenticated user can access other user's profiles without proper authorization checks. Exploiting this vulnerability allows valid users of the system to be listed and sensitive third-party information to be accessed, such as names, email addresses, internal identifiers, and last activity. The endpoint 'http://<IP>:12900/users/<my_user>' does not implement object-level authorization	6.5	More Details

	validations.		
CVE-2026-27057	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Filter Everything penci-filter-everything allows Stored XSS.This issue affects Penci Filter Everything: from n/a through <= 1.7.	6.5	More Details
CVE-2026-27058	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Podcast penci-podcast allows DOM-Based XSS.This issue affects Penci Podcast: from n/a through <= 1.7.	6.5	More Details
CVE-2026-27059	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Recipe penci-recipe allows DOM-Based XSS.This issue affects Penci Recipe: from n/a through <= 4.1.	6.5	More Details
CVE-2026-27069	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Soledad soledad allows DOM-Based XSS.This issue affects Soledad: from n/a through <= 8.7.2.	6.5	More Details
CVE-2026-27092	Missing Authorization vulnerability in Greg Winiarski WPAdverts wpadverts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPAdverts: from n/a through <= 2.2.11.	6.5	More Details
CVE-2026-27094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoDaddy CoBlocks coblocks allows Stored XSS.This issue affects CoBlocks: from n/a through <= 3.1.16.	6.5	More Details
CVE-2026-25307	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore Core et-core-plugin allows DOM-Based XSS.This issue affects XStore Core: from n/a through < 5.7.	6.5	More Details
CVE-2026-1461	The Simple Membership plugin for WordPress is vulnerable to Improper Handling of Missing Values in all versions up to, and including, 4.7.0 via the Stripe webhook handler. This is due to the plugin only validating webhook signatures when the stripe-webhook-signing-secret setting is configured, which is empty by default. This makes it possible for unauthenticated attackers to forge Stripe webhook events to manipulate membership subscriptions, including reactivating expired memberships without payment or canceling legitimate subscriptions, potentially leading to unauthorized access and service disruption.	6.5	More Details
CVE-2025-14799	The Brevo - Email, SMS, Web Push, Chat, and more. plugin for WordPress is vulnerable to authorization bypass due to type juggling in all versions up to, and including, 3.3.0. This is due to the use of loose comparison (==) instead of strict comparison (===) when validating the installation ID in the `/wp-json/mailin/v1/mailin_disconnect` REST API endpoint. This makes it possible for unauthenticated attackers to disconnect the Brevo integration, delete the API key, remove all subscription forms, and reset plugin settings by sending a boolean `true` value for the `id` parameter, which bypasses the authorization check through PHP type juggling.	6.5	More Details
CVE-2026-1942	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the b2s_curation_draft AJAX action in all versions up to, and including, 8.7.4. The curationDraft() function only verifies current_user_can('read') without checking whether the user has edit_post permission for the target post. Combined with the plugin granting UI access and nonce exposure to all roles, this makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the title and content of arbitrary posts and pages by supplying a target post ID via the 'b2s-draft-id' parameter.	6.5	More Details
CVE-2026-25229	Gogs is an open source self-hosted Git service. Versions 0.13.4 and below have a broken access control vulnerability which allows authenticated users with write access to any repository to modify labels belonging to other repositories. The UpdateLabel function in the Web UI (internal/route/repo/issue.go) fails to verify that the label being modified belongs to the repository specified in the URL path, enabling cross-repository label tampering attacks. The vulnerability exists in the Web UI's label update endpoint POST /:username/:reponame/labels/edit. The handler function UpdateLabel uses an incorrect database query function that bypasses repository ownership validation. This issue has been fixed in version 0.14.1.	6.5	More Details
CVE-2025-13587	The Two Factor (2FA) Authentication via Email plugin for WordPress is vulnerable to Two-Factor Authentication Bypass in versions up to, and including, 1.9.8. This is because the SS88_2FAVE::wp_login() method only enforces the 2FA requirement if the 'token' HTTP GET parameter is undefined, which makes it possible to bypass two-factor authentication by supplying any value in the 'token' parameter during login, including an empty one.	6.5	More Details
CVE-2026-0722	The Shield Security plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 21.0.8. This is due to the plugin allowing nonce verification to be bypassed via user-supplied parameter in the 'isNonceVerifyRequired' function. This makes it possible for unauthenticated attackers to execute SQL injection attacks, extracting sensitive information from the database, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2026-2426	The WP-DownloadManager plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.69 via the 'file' parameter in the file deletion functionality. This is due to insufficient validation of user-supplied file paths, allowing directory traversal sequences. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can lead to remote code execution when critical files like wp-config.php are deleted.	6.5	More Details
CVE-2025-13959	The Filestack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'filepicker' shortcode in all versions up to, and including, 2.0.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1373	The Easy Author Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author_profile_picture_url' parameter in all versions up to, and including, 1.7 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-2025-13048	The StatCounter – Free Real Time Visitor Stats plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user's Nickname in all versions up to, and including, 2.1.0 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.	6.4	More Details
CVE-2025-12122	The Popup Box – Easily Create WordPress Popups plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'iframeBox' shortcode in all versions up to, and including, 3.2.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13738	The Easy Table of Contents plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `ez-toc` shortcode in all versions up to, and including, 2.0.78 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0556	The XO Event Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'xo_event_field' shortcode in all versions up to, and including, 3.2.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0549	The Groups plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'groups_group_info' shortcode in all versions up to, and including, 3.10.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2486	The Master Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ma_el_bh_table_btn_text' parameter in versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14983	The Advanced Custom Fields: Font Awesome Field plugin for WordPress is vulnerable to Cross-Site Scripting in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping. This makes it possible forauthenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts that execute in a victim's browser.	6.4	More Details
CVE-2026-1646	The Advance Block Extend plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the TitleColor block attribute in the Latest Posts Gutenberg block in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2384	The Quiz Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `vc_quizmaker` shortcode in all versions up to, and including, 6.7.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note: This vulnerability requires WPBakery Page Builder to be installed and active	6.4	More Details
CVE-2025-14851	The YaMaps for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `yamap` shortcode parameters in all versions up to, and including, 0.6.40 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1941	The WP Event Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wp_events' shortcode in all versions up to, and including, 1.8.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2019-25404	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input through admin management parameters. Attackers can inject script payloads in the admin_name, name, and surname parameters via POST requests to the /korugan/admins endpoint, which are stored and executed when administrators access the interface.	6.4	More Details
CVE-2019-25403	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the comment parameter. Attackers can inject JavaScript code through the admin_profiles endpoint that executes in the browsers of other users who view the affected page.	6.4	More Details
CVE-2025-14445	The Image Hotspot by DevVN plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hotspot_content' custom field meta in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13612	The Album and Image Gallery plus Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `aigpl-gallery-album` shortcode in all versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2718	The Dealia – Request a Quote plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Gutenberg block attributes in all versions up to, and including, 1.0.6. This is due to the use of `wp_kses()` for output escaping within HTML attribute contexts where `esc_attr()` is required. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-	The Apollo13 Framework Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘a13_alt_link’ parameter in all versions up to, and including, 1.9.8 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	6.4	More Details

13617	execute whenever a user accesses an injected page.		
CVE-2025-11185	The Complianz – GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cmplz-accept-link shortcode in all versions up to, and including, 7.4.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6460	The Display During Conditional Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘message’ parameter in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13732	The s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 's2Eot' shortcode in all versions up to, and including, 251005 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-27473	SPIP before 4.4.9 allows Stored Cross-Site Scripting (XSS) via syndicated sites in the private area. The #URL_SYNDIC output is not properly sanitized on the private syndicated site page, allowing an attacker who can set a malicious syndication URL to inject persistent scripts that execute when other administrators view the syndicated site details.	6.4	More Details
CVE-2019-25399	IPFire 2.21 Core Update 127 contains multiple stored cross-site scripting vulnerabilities in the extrahd.cgi script that allow attackers to inject malicious scripts through the FS, PATH, and UUID parameters. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	6.4	More Details
CVE-2025-12375	The Printful Integration for WooCommerce plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.2.11 via the advanced size chart REST API endpoint. This is due to insufficient validation of user-supplied URLs before passing them to the download_url() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application which can be used to query and modify information from internal services.	6.4	More Details
CVE-2025-11737	The VK All in One Expansion Unit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vkExUnit_sns_title' parameter in all versions up to, and including, 9.112.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12117	The Renden theme for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in all versions up to, and including, 1.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-23803	Server-Side Request Forgery (SSRF) vulnerability in Burhan Nasir Smart Auto Upload Images smart-auto-upload-images allows Server Side Request Forgery.This issue affects Smart Auto Upload Images: from n/a through <= 1.2.2.	6.4	More Details
CVE-2019-25448	OrientDB 3.0.17 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by creating users with script payloads in the name parameter. Attackers can send POST requests to the document endpoint with JavaScript code in the name field to execute arbitrary scripts when users view the application.	6.4	More Details
CVE-2026-1807	The InteractiveCalculator for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'interactivecalculator' shortcode in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12448	The Smartsupp – live chat, AI shopping assistant and chatbots plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'code' parameter in all versions up to, and including, 3.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12116	The Drift theme for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in all versions up to, and including, 1.5.0 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.	6.4	More Details
CVE-2026-2977	A security vulnerability has been detected in FastApiAdmin up to 2.2.0. This affects the function upload_controller of the file /backend/app/api/v1/module_common/file/controller.py of the component Scheduled Task API. Such manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-2682	A vulnerability has been found in Tsinghua Unigroup Electronic Archives System up to 3.2.210802(62532). Impacted is an unknown function of the file /mine/PublicReport/prinReport.html?token=java. Such manipulation of the argument comid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2978	A vulnerability was detected in FastApiAdmin up to 2.2.0. This vulnerability affects the function upload_file_controller of the file /backend/app/api/v1/module_system/params/controller.py of the component Scheduled Task API. Performing a manipulation results in unrestricted upload. The attack can be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-3065	A vulnerability was detected in HummerRisk up to 1.5.0. This affects the function CommandUtils.commonExecCmdWithResult of the file CloudTaskService.java of the component Cloud Task Dry-run. Performing a manipulation of the argument fileName results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The	6.3	More Details

	vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-2676	A weakness has been identified in GoogTech sms-ssm up to e8534c766fd13f5f94c01dab475d75f286918a8d. Affected by this issue is the function preHandle of the file LoginInterceptor.java of the component API Interface. Executing a manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	6.3	More Details
CVE-2026-2979	A flaw has been found in FastApiAdmin up to 2.2.0. This issue affects the function user_avatar_upload_controller of the file /backend/app/api/v1/module_system/user/controller.py of the component Scheduled Task API. Executing a manipulation can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-2435	Tanium addressed a SQL injection vulnerability in Asset.	6.3	More Details
CVE-2026-27113	Liquid Prompt is an adaptive prompt for Bash and Zsh. Starting in commit cf3441250bb5d8b45f6f8b389fcdf427a99ac28a and prior to commit a4f6b8d8c90b3eaa33d13dfd1093062ab9c4b30c on the master branch, arbitrary command injection can lead to code execution when a user enters a directory in a Git repository containing a crafted branch name. Exploitation requires the LP_ENABLE_GITSTATUSD config option to be enabled (enabled by default), gitstatusd to be installed and started before Liquid Prompt is loaded (not the default), and shell prompt substitution to be active (enabled by default in Bash via "shopt -s promptvars", not enabled by default in Zsh). A branch name containing shell syntax such as "$(...)" or backtick expressions in the default branch or a checked-out branch will be evaluated by the shell when the prompt is rendered. No stable release is affected; only the master branch contains the vulnerable commit. Commit a4f6b8d8c90b3eaa33d13dfd1093062ab9c4b30c contains a fix. As a workaround, set the LP_ENABLE_GITSTATUSD config option to 0.	6.3	More Details
CVE-2026-2654	A weakness has been identified in huggingface smolagents 1.24.0. Impacted is the function requests.get/requests.post of the component LocalPythonExecutor. Executing a manipulation can lead to server-side request forgery. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2819	A vulnerability was identified in Dromara RuoYi-Vue-Plus up to 5.5.3. This vulnerability affects the function SaServletFilter of the file /workflow/instance/deleteByInstanceIds of the component Workflow Module. The manipulation leads to missing authorization. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3067	A vulnerability has been found in HummerRisk up to 1.5.0. This issue affects the function extractTarGZ/extractZip of the file hummer-common/hummer-common-core/src/main/java/com/hummer/common/core/utils/CommandUtils.java of the component Archive Extraction. The manipulation leads to path traversal. 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.	6.3	More Details
CVE-2026-2963	A vulnerability was determined in Jinher OA C6 up to 20260210. This issue affects some unknown processing of the file /C6/Jhsoft.Web.officesupply/OfficeSupplyTypeRight.aspx. This manipulation of the argument id/offsnum causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. It is suggested to install a patch to address this issue. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2956	A security flaw has been discovered in qinming99 dst-admin up to 1.5.0. This affects the function revertBackup of the file /home/restore. The manipulation of the argument Name results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3066	A flaw has been found in HummerRisk up to 1.5.0. This vulnerability affects the function fixedCommand of the file hummer-common/hummer-common-core/src/main/java/com/hummer/common/core/utils/PlatformUtils.java of the component Cloud Compliance Scanning. Executing a manipulation can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-68022	Missing Authorization vulnerability in soporteblue Plugin BlueX for WooCommerce bluex-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Plugin BlueX for WooCommerce: from n/a through <= 3.1.6.	6.3	More Details
CVE-2026-2954	A vulnerability was found in Dromara UJCMS 10.0.2. Impacted is the function importChanel of the file /api/backend/ext/import-data/import-channel of the component ImportDataController. Performing a manipulation of the argument driverClassName/url results in injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2665	A vulnerability was detected in huanzi-qch base-admin up to 57a8126bb3353a004f3c7722089e3b926ea83596. Impacted is the function Upload of the file SysFileController.java of the component JSP Parser. Performing a manipulation of the argument File results in unrestricted upload. The attack can be initiated remotely. The exploit is now public 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 project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2663	A security vulnerability has been detected in Alixhan xh-admin-backend up to 1.7.0. This issue affects some unknown processing of the file /frontend-api/system-service/api/system/role/query of the component Database Query Handler. Such manipulation of the argument prop leads to sql injection. It is possible to launch 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.	6.3	More Details
CVE-2026-1200	A flaw was found in the rgaufman/live555 fork of live555. A remote attacker could exploit a segmentation fault, in the `increaseBufferTo` function. This vulnerability can lead to memory corruption problems and potentially other consequences.	6.3	More Details

CVE-2026-2850	A vulnerability was found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This affects the function addCustomer/updateCustomer/deleteCustomer of the file dataset\repos\warehouse\src\main\java\com\yeqifu\bus\controller\CustomerController.java of the component Customer Endpoint. Performing a manipulation results in improper access controls. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2851	A vulnerability was determined in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This vulnerability affects the function addInport/updateInport/deleteInport of the file dataset\repos\warehouse\src\main\java\com\yeqifu\bus\controller\InportController.java of the component Inport Endpoint. Executing a manipulation can lead to improper access controls. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2985	A security flaw has been discovered in Tiandy Video Surveillance System 视频监控平台 7.17.0. This impacts the function downloadImage of the file /com/tiandy/easy7/core/bo/CLSBODownLoad.java. Performing a manipulation of the argument urlPath results in server-side request forgery. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3052	A vulnerability was found in DataLinkDC dinky up to 1.2.5. The impacted element is the function proxyUba of the file dinky-admin/src/main/java/org/dinky/controller/FlinkProxyController.java of the component Flink Proxy Controller. Performing a manipulation results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2860	A security vulnerability has been detected in feng_ha_ha/megagao ssm-erp and production_ssm up to 4288d53bd35757b27f2d070057aefb2c07bdd097. Impacted is an unknown function of the file EmployeeController.java. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. This product is distributed under two entirely different names. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2852	A vulnerability was identified in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This issue affects the function addSales/updateSales/deleteSales of the file dataset\repos\warehouse\src\main\java\com\yeqifu\bus\controller\SalesController.java of the component Sales Endpoint. The manipulation leads to improper access controls. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-3057	A security flaw has been discovered in a54552239 pearProjectApi up to 2.8.10. Affected is the function dateTotalForProject of the file application/common/Model/Task.php of the component Backend Interface. The manipulation of the argument projectCode results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3102	A vulnerability was determined in exiftool up to 13.49 on macOS. This issue affects the function SetMacOSTags of the file lib/Image/ExifTool/MacOS.pm of the component PNG File Parser. This manipulation of the argument DateTimeOriginal causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 13.50 is capable of addressing this issue. Patch name: e9609a9bcc0d32bd252a709a562fb822d6dd86f7. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-2930	A vulnerability was identified in Tenda A18 15.13.07.13. The affected element is the function webCgiGetUploadFile of the file /cgi-bin/UploadCfg of the component Httpd Service. Such manipulation of the argument boundary leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-2945	A weakness has been identified in JeecgBoot 3.9.0. Affected by this vulnerability is an unknown functionality of the file /sys/common/uploadImgByHttp. Executing a manipulation of the argument fileUrl can lead to server-side request forgery. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3064	A security vulnerability has been detected in HummerRisk up to 1.5.0. Affected by this issue is some unknown functionality of the file ResourceCreateService.java of the component Cloud Task Scheduler. Such manipulation of the argument regionId leads to command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-3051	A vulnerability has been found in DataLinkDC dinky up to 1.2.5. The affected element is the function getProjectDir of the file dinky-admin/src/main/java/org/dinky/utils/GitRepository.java of the component Project Name Handler. Such manipulation of the argument projectName leads to path traversal. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2824	A flaw has been found in Comfast CF-E7 2.6.0.9. This affects the function sub_441CF4 of the file /cgi-bin/mbox-config?method=SET&section=ping_config of the component webmggnt. Executing a manipulation of the argument destination can lead to command injection. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2823	A vulnerability was detected in Comfast CF-E7 2.6.0.9. The impacted element is the function sub_41ACCC of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone of the component webmggnt. Performing a manipulation of the argument timestr results in command injection. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-	A security vulnerability has been detected in JeecgBoot up to 3.9.1. The affected element is an unknown function of the file		

2026-2822	/jeecgboot/sys/dict/loadDict/airag_app,1,create_by of the component Backend Interface. Such manipulation of the argument keyword leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-2706	A flaw has been found in code-projects Patient Record Management System 1.0. This affects an unknown function of the file /fecalysis_not.php. This manipulation of the argument comp_id causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-3101	A vulnerability was found in Intelbras TIP 635G 1.12.3.5. This vulnerability affects unknown code of the component Ping Handler. The manipulation results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-8308	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Key Software Solutions Inc. INFOREX- General Information Management System allows XSS Through HTTP Headers.This issue affects INFOREX- General Information Management System: from 2025 and before through 18022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2697	An Indirect Object Reference (IDOR) in Security Center allows an authenticated remote attacker to escalate privileges via the 'owner' parameter.	6.3	More Details
CVE-2026-22268	Dell PowerProtect Data Manager, version(s) prior to 19.22, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to denial of service of a Dell Enterprise Support connection.	6.3	More Details
CVE-2026-26283	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a `continue` statement in the JPEG extent binary search loop in the jpeg encoder causes an infinite loop when writing persistently fails. An attacker can trigger a 100% CPU consumption and process hang (Denial of Service) with a crafted image. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.2	More Details
CVE-2025-61147	strukturag libde265 commit d9fea9d wa discovered to contain a segmentation fault via the component decoder_context::compute_framedrop_table().	6.2	More Details
CVE-2026-25971	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, Magick fails to check for circular references between two MSLs, leading to a stack overflow. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.2	More Details
CVE-2026-26066	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a crafted profile contain invalid IPTC data may cause an infinite loop when writing it with `IPTCTEXT`. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	6.2	More Details
CVE-2019-25326	ipPulse 1.92 contains a denial of service vulnerability that allows local attackers to crash the application by providing an oversized input in the Enter Key field. Attackers can generate a 256-byte buffer of repeated 'A' characters to trigger an application crash when pasting the malicious content.	6.2	More Details
CVE-2019-25437	Foscam Video Management System 1.1.6.6 contains a buffer overflow vulnerability in the UID field that allows local attackers to crash the application by supplying an excessively long string. Attackers can input a 5000-character buffer into the UID parameter during device addition to trigger an application crash when the Login Check function is invoked.	6.2	More Details
CVE-2026-0561	The Shield Security plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'message' parameter in all versions up to, and including, 21.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-71244	SPIP before 4.4.5 and 4.3.9 allows an Open Redirect via the login form when used in AJAX mode. An attacker can craft a malicious URL that, when visited by a victim, redirects them to an arbitrary external site after login. This vulnerability only affects sites where the login page has been overridden to function in AJAX mode. It is not mitigated by the SPIP security screen.	6.1	More Details
CVE-2025-11706	The Aruba HiSpeed Cache plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the dbstatus parameter in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-1666	The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'redirect_to' parameter in all versions up to, and including, 3.3.46. This is due to insufficient input sanitization and output escaping on the 'redirect_to' GET parameter in the login form shortcode. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2019-25412	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input through the NTP_SERVER_LIST parameter. Attackers can send POST requests to the /korugan/time endpoint with script payloads in the NTP_SERVER_LIST parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25411	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the GATEWAY_GREEN parameter. Attackers can send POST requests to the DHCP configuration endpoint with script payloads to execute arbitrary JavaScript in administrator browsers.	6.1	More Details
CVE-2019-25423	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the /korugan/proxyconfig endpoint that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted POST requests with JavaScript payloads in parameters like PROXY_PORT, VISIBLE_HOSTNAME, ADMIN_MAIL_ADDRESS, CACHE_MEM, MAX_SIZE, MIN_SIZE, and DST_NOCACHE to execute arbitrary scripts in administrator browsers.	6.1	More Details

CVE-2026-27120	Leafkit is a templating language with Swift-inspired syntax. Prior to 1.4.1, htmlEscaped in leaf-kit will only escape html special characters if the extended grapheme clusters match, which allows bypassing escaping by using an extended grapheme cluster containing both the special html character and some additional characters. In the case of html attributes, this can lead to XSS if there is a leaf variable in the attribute that is user controlled. This vulnerability is fixed in 1.4.1.	6.1	More Details
CVE-2019-25424	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the EXCEPTIONSITELIST parameter. Attackers can craft POST requests to the https_exceptions endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	6.1	More Details
CVE-2019-25410	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts through the source and destination parameters. Attackers can submit POST requests to the policy routing endpoint with script payloads in these parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25409	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the destination parameter. Attackers can send POST requests to the routing endpoint with script payloads in the destination parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25427	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the antispyware endpoint. Attackers can send POST requests with JavaScript payloads in the DNSMASQ_WHITELIST or DNSMASQ_BLACKLIST parameters to execute arbitrary code in users' browsers.	6.1	More Details
CVE-2019-25407	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the backup schedule interface. Attackers can send POST requests to the backupschedule endpoint with JavaScript code in the BACKUP_RCPTTO parameter to execute arbitrary scripts in users' browsers.	6.1	More Details
CVE-2026-27506	SVXportal version 2.5 and prior contain a stored cross-site scripting vulnerability in the user profile update workflow (user_settings.php submitting to admin/update_user.php). Authenticated users can store malicious HTML/JavaScript in fields such as Firstname, lastname, email, and image_url, which are later rendered without adequate output encoding in the administrator interface (admin/users.php), resulting in JavaScript execution in an administrator's browser when the affected page is viewed.	6.1	More Details
CVE-2019-25413	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the ID parameter. Attackers can craft requests to the /manage/ips/rules/ endpoint with script payloads in the ID parameter to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2026-27512	Shenzhen Tenda F3 Wireless Router firmware V12.01.01.55_multi contains a content-type confusion vulnerability in the administrative interface. Responses omit the X-Content-Type-Options: nosniff header and include attacker-influenced content that can be reflected into the response body. Under affected browser behaviors, MIME sniffing may cause the response to be interpreted as active HTML, enabling script execution in the context of the administrative interface.	6.1	More Details
CVE-2025-67438	A Stored Cross-Site Scripting (XSS) vulnerability in Sync-in Server before 1.9.3 allows an authenticated attacker to execute arbitrary JavaScript in a victim's browser. By uploading a crafted SVG file containing a malicious payload, an attacker can access and exfiltrate sensitive information, including the user's session cookies.	6.1	More Details
CVE-2026-27505	SVXportal version 2.5 and prior contain a stored cross-site scripting vulnerability in the user registration workflow (index.php submitting to admin/user_action.php). User-supplied fields such as Firstname, lastname, and email are stored in the backend database without adequate output encoding and are later rendered in the administrator interface (admin/users.php), allowing an unauthenticated remote attacker to inject arbitrary JavaScript that executes in an administrator's browser upon viewing the affected page.	6.1	More Details
CVE-2019-25396	IPFire 2.21 Core Update 127 contains a reflected cross-site scripting vulnerability in the updatexlrator.cgi script that allows attackers to inject malicious scripts through POST parameters. Attackers can submit crafted requests with script payloads in the MAX_DISK_USAGE or MAX_DOWNLOAD_RATE parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2025-12451	The Easy SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file uploads in all versions up to, and including, 4.0 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 the SVG file.	6.1	More Details
CVE-2019-25397	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the KEY1, IP, HOST, or DOM parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25398	IPFire 2.21 Core Update 127 contains multiple cross-site scripting vulnerabilities in the ovpnmain.cgi script that allow attackers to inject malicious scripts through VPN configuration parameters. Attackers can submit POST requests with script payloads in parameters like VPN_IP, DMTU, ccdname, ccdsubnet, DOVPN_SUBNET, DHCP_DOMAIN, DHCP_DNS, DHCP_WINS, ROUTES_PUSH, FRAGMENT, KEEPALIVE_1, and KEEPALIVE_2 to execute arbitrary JavaScript in administrator browsers.	6.1	More Details
CVE-2025-62326	HCL Digital Experience is susceptible to stored cross-site scripting (XSS) in the administrative user interface which would require elevated privileges to exploit.	6.1	More Details
CVE-2026-2502	The xmlrpc attacks blocker plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 1.0, via the 'X-Forwarded-For' HTTP header. This is due to the plugin trusting and logging attacker-controlled IP header data and rendering debug log entries without output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the debug log page.	6.1	More Details
CVE-2019-25428	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the openvpn_users endpoint that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted POST requests with script payloads in the username, remotenets, explicitroutes, static_ip, custom_dns, or custom_domain parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-	Comodo Dome Firewall 2.7.0 contains multiple cross-site scripting vulnerabilities that allow attackers to inject malicious scripts		

2019-25421	through the policyfw endpoint. Attackers can submit POST requests with JavaScript payloads in the mac, target, and remark parameters to execute arbitrary code in administrator browsers or store persistent scripts in the application.	6.1	More Details
CVE-2019-25420	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the snat endpoint. Attackers can send POST requests with JavaScript payloads in the port or snat_to_ip parameters to execute arbitrary scripts in users' browsers.	6.1	More Details
CVE-2019-25429	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the openvpn_advanced endpoint. Attackers can inject JavaScript code through the GLOBAL_NETWORKS and GLOBAL_DNS parameters via POST requests to execute arbitrary scripts in users' browsers.	6.1	More Details
CVE-2019-25418	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the FWADDRESSES parameter. Attackers can send POST requests to the /korugan/fwgroups endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	6.1	More Details
CVE-2019-25417	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the protocol parameter. Attackers can send POST requests to the QoS rules management endpoint with JavaScript payloads in the protocol parameter to execute arbitrary code in administrator browsers.	6.1	More Details
CVE-2019-25416	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through the device parameter. Attackers can send POST requests to the QoS devices management endpoint with script payloads in the device parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25415	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the hotspot_permanent_users endpoint. Attackers can send POST requests with JavaScript payloads in the MACADDRESSES parameter to execute arbitrary scripts in users' browsers.	6.1	More Details
CVE-2019-25414	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the ID parameter. Attackers can craft requests to the /manage/ips/appid/ endpoint with script payloads in the ID parameter to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2019-25445	Fiverr Clone Script 1.2.2 contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the keyword parameter. Attackers can craft URLs with script tags in the keyword parameter of search-results.php to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25430	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter. Attackers can send POST requests to the vpn_users endpoint with script payloads in the username field to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2019-25425	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the VIRUS_ADMIN parameter. Attackers can send POST requests to the smtpconfig endpoint with script payloads to execute arbitrary JavaScript in the context of an administrator's browser session.	6.1	More Details
CVE-2019-25408	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the netmask_addr parameter. Attackers can send POST requests to the netwizard2 endpoint with script payloads in the netmask_addr parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2026-26464	Stored Cross-Site Scripting (XSS) was found in the /admin/edit_user.php page of Society Management System Portal V1.0, which allows remote attackers to inject and store arbitrary JavaScript code that is executed in users' browsers. This vulnerability can be exploited via the name parameter in a POST HTTP request, leading to execution of malicious scripts when the affected content is viewed by other users, including administrators.	6.1	More Details
CVE-2026-1440	Reflected Cross-Site Scripting (XSS) vulnerability in the Graylog Web Interface console, version 2.2.3, caused by a lack of proper sanitization and escaping in HTML output. Several endpoints include segments of the URL directly in the response without applying output encoding, allowing an attacker to inject and execute arbitrary JavaScript code when a user visits a specially crafted URL. Exploitation of this vulnerability may allow script execution in the victim's browser and limited manipulation of the affected user's session context, through the '/system/pipelines/' endpoint.	6.1	More Details
CVE-2025-14076	The iXML – Google XML sitemap generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'iXML_email' parameter in all versions up to, and including, 0.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-1439	Reflected Cross-Site Scripting (XSS) vulnerability in the Graylog Web Interface console, version 2.2.3, caused by a lack of proper sanitization and escaping in HTML output. Several endpoints include segments of the URL directly in the response without applying output encoding, allowing an attacker to inject and execute arbitrary JavaScript code when a user visits a specially crafted URL. Exploitation of this vulnerability may allow script execution in the victim's browser and limited manipulation of the affected user's session context, through the '/ alerts /' endpoint.	6.1	More Details
CVE-2025-15562	The server API endpoint /report/internet/urls reflects received data into the HTML response without applying proper encoding or filtering. This allows an attacker to execute arbitrary JavaScript in the victim's browser if the victim opens a URL prepared by the attacker.	6.1	More Details
CVE-2026-1296	The Frontend Post Submission Manager Lite plugin for WordPress is vulnerable to Open Redirection in all versions up to, and including, 1.2.7 due to insufficient validation on the 'requested_page' POST parameter in the verify_username_password function. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action such as clicking on a link.	6.1	More Details
CVE-2019-25356	Bematech (formerly Logic Controls, now Elgin) MP-4200 TH printer contains a cross-site scripting vulnerability in the admin configuration page. Attackers can inject malicious scripts via crafted POST requests with malformed 'admin' and 'person' parameters, allowing execution of arbitrary JavaScript in the context of an authenticated user's browser session.	6.1	More Details

CVE-2026-26987	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below are vulnerable to Reflected XSS attacks via email field. This issue has been fixed in version 26.2.0.	6.1	More Details
CVE-2026-27469	Isso is a lightweight commenting server written in Python and JavaScript. In commits before 0afbfe0691ee237963e8fb0b2ee01c9e55ca2144, there is a stored Cross-Site Scripting (XSS) vulnerability affecting the website and author comment fields. The website field was HTML-escaped using quote=False, which left single and double quotes unescaped. Since the frontend inserts the website value directly into a single-quoted href attribute via string concatenation, a single quote in the URL breaks out of the attribute context, allowing injection of arbitrary event handlers (e.g. onmouseover, onclick). The same escaping is missing entirely from the user-facing comment edit endpoint (PUT /id/) and the moderation edit endpoint (POST /id//edit/). This issue has been patched in commit 0afbfe0691ee237963e8fb0b2ee01c9e55ca2144. To workaround, nabling comment moderation (moderation = enabled = true in isso.cfg) prevents unauthenticated users from publishing comments, raising the bar for exploitation, but it does not fully mitigate the issue since a moderator activating a malicious comment would still expose visitors.	6.1	More Details
CVE-2019-25402	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter. Attackers can send POST requests to the login endpoint with script payloads in the username field to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25453	phpMoAdmin 1.1.5 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the newdb parameter. Attackers can craft URLs with JavaScript payloads in the newdb parameter of moadmin.php to execute arbitrary code in users' browsers when they visit the malicious link.	6.1	More Details
CVE-2019-25406	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the organization parameter. Attackers can send POST requests to the korugan/cmclient endpoint with script payloads in the organization parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2026-1404	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the filter parameters (e.g., 'filter_first_name') in all versions up to, and including, 2.11.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2019-25449	OrientDB 3.0.17 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted JSON payloads to the document endpoint. Attackers can send POST requests to /document/demodb/-1:-1 with script tags in the name parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25426	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the dnsmasq endpoint. Attackers can send POST requests with script payloads in the TRANSPARENT_SOURCE_BYPASS or TRANSPARENT_DESTINATION_BYPASS parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2026-27502	SVXportal version 2.5 and prior contain a reflected cross-site scripting vulnerability in log.php via the search query parameter. The application embeds the unsanitized parameter value directly into an HTML input value attribute, allowing an unauthenticated remote attacker to inject and execute arbitrary JavaScript in a victim's browser if the victim visits a crafted URL. This can be used to steal session data, perform actions as the victim, or modify displayed content.	6.1	More Details
CVE-2026-27503	SVXportal version 2.5 and prior contain a reflected cross-site scripting vulnerability in admin/log.php via the search query parameter. When an authenticated administrator views a crafted URL, the application embeds the unsanitized parameter value directly into an HTML input value attribute, allowing attacker-supplied JavaScript to execute in the administrator's browser. This can enable session theft, administrative action forgery, or other browser-based compromise in the context of an admin user.	6.1	More Details
CVE-2026-27504	SVXportal version 2.5 and prior contain a reflected cross-site scripting vulnerability in radiomobile_front.php via the stationid query parameter. When an authenticated administrator views a crafted URL, the application embeds the unsanitized parameter value into a hidden input value field, allowing attacker-supplied script injection and execution in the administrator's browser. This can be used to compromise admin sessions or perform unauthorized actions via the administrator's authenticated context.	6.1	More Details
CVE-2026-26963	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Versions 1.18.0 through 1.18.5 will incorrectly permit traffic from Pods on other nodes when Native Routing, WireGuard and Node Encryption are enabled. This issue has been fixed in version 1.18.6.	6.1	More Details
CVE-2026-27156	NiceGUI is a Python-based UI framework. Prior to version 3.8.0, several NiceGUI APIs that execute methods on client-side elements (`Element.run_method()`, `AgGrid.run_grid_method()`, `EChart.run_chart_method()`, and others) use an `eval()` fallback in the JavaScript-side `runMethod()` function. When user-controlled input is passed as the method name, an attacker can inject arbitrary JavaScript that executes in the victim's browser. Additionally, `Element.run_method()` and `Element.get_computed_prop()` used string interpolation instead of `json.dumps()` for the method/property name, allowing quote injection to break out of the intended string context. Version 3.8.0 contains a fix.	6.1	More Details
CVE-2026-27176	MajorDoMo (aka Major Domestic Module) contains a reflected cross-site scripting (XSS) vulnerability in command.php. The $qry parameter is rendered directly into the HTML page without sanitization via htmlspecialchars(), both in an input field value attribute and in a paragraph element. An attacker can inject arbitrary JavaScript by crafting a URL with malicious content in the qry parameter.	6.1	More Details
CVE-2026-1437	Reflected Cross-Site Scripting (XSS) vulnerability in the Graylog Web Interface console, version 2.2.3, caused by a lack of proper sanitization and escaping in HTML output. Several endpoints include segments of the URL directly in the response without applying output encoding, allowing an attacker to inject and execute arbitrary JavaScript code when a user visits a specially crafted URL. Exploitation of this vulnerability may allow script execution in the victim's browser and limited manipulation of the affected user's session context, through the '/system/authentication/users/edit/' endpoint.	6.1	More Details
CVE-	Reflected Cross-Site Scripting (XSS) vulnerability in the Graylog Web Interface console, version 2.2.3, caused by a lack of proper sanitization and escaping in HTML output. Several endpoints include segments of the URL directly in the response without		More

2026-1438	applying output encoding, allowing an attacker to inject and execute arbitrary JavaScript code when a user visits a specially crafted URL. Exploitation of this vulnerability may allow script execution in the victim's browser and limited manipulation of the affected user's session context, through the '/system/nodes/' endpoint.	6.1	Details
CVE-2026-2736	Reflected Cross-site Scripting (XSS) in Alkacon's OpenCms v18.0, which allows an attacker to execute JavaScript code in the victim's browser by sending the victim a malicious URL containing the 'q' parameter in '/search/index.html'. This vulnerability can be exploited to steal sensitive user information such as session cookies, or to perform actions while impersonating the user.	6.1	More Details
CVE-2025-46320	A cross-site scripting (XSS) vulnerability in a FileMaker WebDirect custom homepage could lead to unauthorized access and remote code execution. This vulnerability has been fully addressed in FileMaker Server 22.0.4 and FileMaker Server 21.1.7.	6.1	More Details
CVE-2026-1441	Reflected Cross-Site Scripting (XSS) vulnerability in the Graylog Web Interface console, version 2.2.3, caused by a lack of proper sanitization and escaping in HTML output. Several endpoints include segments of the URL directly in the response without applying output encoding, allowing an attacker to inject and execute arbitrary JavaScript code when a user visits a specially crafted URL. Exploitation of this vulnerability may allow script execution in the victim's browser and limited manipulation of the affected user's session context, through the '/system/index_sets/' endpoint.	6.1	More Details
CVE-2026-24392	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nabil Lemsieh HurryTimer hurrytimer allows Stored XSS.This issue affects HurryTimer: from n/a through <= 2.14.2.	5.9	More Details
CVE-2025-59873	An information exposure vulnerability exists in Vulnerability in HCL Software ZIE for Web. The application transmits sensitive session tokens and authentication identifiers within the URL query parameters . An attacker who gains access to any network log or operates a site linked from the application can hijack user sessions This issue affects ZIE for Web: v16.	5.9	More Details
CVE-2026-25966	ImageMagick is free and open-source software used for editing and manipulating digital images. The shipped "secure" security policy includes a rule intended to prevent reading/writing from standard streams. However, ImageMagick also supports fd:<n> pseudo-filenames (e.g., fd:0, fd:1). Prior to versions 7.1.2-15 and 6.9.13-40, this path form is not blocked by the secure policy templates, and therefore bypasses the protection goal of "no stdin/stdout." Versions 7.1.2-15 and 6.9.13-40 contain a patch by including a change to the more secure policies by default. As a workaround, add the change to one's security policy manually.	5.9	More Details
CVE-2026-27482	Ray is an AI compute engine. In versions 2.53.0 and below, thedashboard HTTP server blocks browser-origin POST/PUT but does not cover DELETE, and key DELETE endpoints are unauthenticated by default. If the dashboard/agent is reachable (e.g., --dashboard-host=0.0.0.0), a web page via DNS rebinding or same-network access can issue DELETE requests that shut down Serve or delete jobs without user interaction. This is a drive-by availability impact. The fix for this vulnerability is to update to Ray 2.54.0 or higher.	5.9	More Details
CVE-2026-27133	Strimzi provides a way to run an Apache Kafka cluster on Kubernetes or OpenShift in various deployment configurations. From 0.47.0 to before 0.50.1, when a chain consisting of multiple CA (Certificate Authority) certificates is used in the trusted certificates configuration of a Kafka Connect operand or of the target cluster in the Kafka MirrorMaker 2 operand, all of the certificates that are part of the CA chain will be trusted individually when connecting to the Apache Kafka cluster. Due to this error, the affected operand (Kafka Connect or Kafka MirrorMaker 2) might accept connections to Kafka brokers using server certificates signed by one of the other CAs in the CA chain and not just by the last CA in the chain. This issue is fixed in Strimzi 0.50.1.	5.9	More Details
CVE-2026-25362	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FooPlugins FooGallery foogallery allows Stored XSS.This issue affects FooGallery: from n/a through <= 3.1.11.	5.9	More Details
CVE-2026-27729	Astro is a web framework. In versions 9.0.0 through 9.5.3, Astro server actions have no default request body size limit, which can lead to memory exhaustion DoS. A single large POST to a valid action endpoint can crash the server process on memory-constrained deployments. On-demand rendered sites built with Astro can define server actions, which automatically parse incoming request bodies (JSON or FormData). The body is buffered entirely into memory with no size limit — a single oversized request is sufficient to exhaust the process heap and crash the server. Astro's Node adapter (`mode: 'standalone'`) creates an HTTP server with no body size protection. In containerized environments, the crashed process is automatically restarted, and repeated requests cause a persistent crash-restart loop. Action names are discoverable from HTML form attributes on any public page, so no authentication is required. The vulnerability allows unauthenticated denial of service against SSR standalone deployments using server actions. A single oversized request crashes the server process, and repeated requests cause a persistent crash-restart loop in containerized environments. Version 9.5.4 contains a fix.	5.9	More Details
CVE-2026-27360	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10Web Photo Gallery by 10Web photo-gallery allows Stored XSS.This issue affects Photo Gallery by 10Web: from n/a through <= 1.8.37.	5.9	More Details
CVE-2026-27368	Missing Authorization vulnerability in SeedProd Coming Soon Page, Under Construction & Maintenance Mode by SeedProd coming-soon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Coming Soon Page, Under Construction & Maintenance Mode by SeedProd: from n/a through <= 6.19.7.	5.9	More Details
CVE-2026-27571	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. The WebSockets handling of NATS messages handles compressed messages via the WebSockets negotiated compression. Prior to versions 2.11.2 and 2.12.3, the implementation bound the memory size of a NATS message but did not independently bound the memory consumption of the memory stream when constructing a NATS message which might then fail validation for size reasons. An attacker can use a compression bomb to cause excessive memory consumption, often resulting in the operating system terminating the server process. The use of compression is negotiated before authentication, so this does not require valid NATS credentials to exploit. The fix, present in versions 2.11.2 and 2.12.3, was to bounds the decompression to fail once the message was too large, instead of continuing on. The vulnerability only affects deployments which use WebSockets and which expose the network port to untrusted end-points.	5.9	More Details
	Trivy Action runs Trivy as GitHub action to scan a Docker container image for vulnerabilities. A command injection vulnerability exists in `aquasecurity/trivy-action` versions 0.31.0 through 0.33.1 due to improper handling of action inputs when exporting		

CVE-2026-26189	environment variables. The action writes `export VAR=<input>` lines to `trivy_envs.txt` based on user-supplied inputs and subsequently sources this file in `entrypoint.sh`. Because input values are written without appropriate shell escaping, attacker-controlled input containing shell metacharacters (e.g., `$(...)`, backticks, or other command substitution syntax) may be evaluated during the sourcing process. This can result in arbitrary command execution within the GitHub Actions runner context. Version 0.34.0 contains a patch for this issue. The vulnerability is exploitable when a consuming workflow passes attacker-controlled data into any action input that is written to `trivy_envs.txt`. Access to user input is required by the malicious actor. Workflows that do not pass attacker-controlled data into `trivy-action` inputs, workflows that upgrade to a patched version that properly escapes shell values or eliminates the `source ./trivy_envs.txt` pattern, and workflows where user input is not accessible are not affected.	5.9	More Details
CVE-2026-25343	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS wp-sms allows DOM-Based XSS.This issue affects WP SMS: from n/a through <= 7.1.	5.9	More Details
CVE-2026-27009	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a atored XSS issue in the OpenClaw Control UI when rendering assistant identity (name/avatar) into an inline `<script>` tag without script-context-safe escaping. A crafted value containing `</script>` could break out of the script tag and execute attacker-controlled JavaScript in the Control UI origin. Version 2026.2.15 removed inline script injection and serve bootstrap config from a JSON endpoint and added a restrictive Content Security Policy for the Control UI (`script-src 'self'`, no inline scripts).	5.8	More Details
CVE-2026-24746	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the Edit Quotes functions of InvoicePlane version 1.7.0. In the Editing Quotes function, the application does not validate user input at the quote_number parameter. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	5.7	More Details
CVE-2026-24743	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the upload Invoice Logo functions of InvoicePlane version 1.7.0. The Upload Invoice Logo function allows the application to upload svg files. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	5.7	More Details
CVE-2026-24744	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the Edit Invoices functions of InvoicePlane version 1.7.0. When editing invoices, the application does not validate user input at the `invoice_number` parameter. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	5.7	More Details
CVE-2026-26049	The web management interface of the device renders the passwords in a plaintext input field. The current password is directly visible to anyone with access to the UI, potentially exposing administrator credentials to unauthorized observation via shoulder surfing, screenshots, or browser form caching.	5.7	More Details
CVE-2026-24745	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the upload Login Logo functions of InvoicePlane version 1.7.0. In the Upload Login Logo, the application allows uploading svg files. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	5.7	More Details
CVE-2026-25797	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, the ps coders, responsible for writing PostScript files, fails to sanitize the input before writing it into the PostScript header. An attacker can provide a malicous file and inject arbitrary PostScript code. When the resulting file is processed by a printer or a viewer (like Ghostscript), the injected code is interpreted and executed. The html encoder does not properly escape strings that are written to in the html document. An attacker can provide a malicious file and injection arbitrary html code. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.7	More Details
CVE-2026-2711	A vulnerability has been found in zhutoutoutousan worldquant-miner up to 1.0.9. The impacted element is an unknown function of the file worldquant-miner-master/agent-dify-api/core/helper/ssrf_proxy.py of the component URL Handler. The manipulation of the argument make_request leads to server-side request forgery. The attack can be initiated remotely. The attack's complexity is rated as high. The exploitability is regarded as difficult. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.6	More Details
CVE-2026-27004	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, in some shared-agent deployments, OpenClaw session tools (`sessions_list`, `sessions_history`, `sessions_send`) allowed broader session targeting than some operators intended. This is primarily a configuration/visibility-scoping issue in multi-user environments where peers are not equally trusted. In Telegram webhook mode, monitor startup also did not fall back to per-account `webhookSecret` when only the account-level secret was configured. In shared-agent, multi-user, less-trusted environments: session-tool access could expose transcript content across peer sessions. In single-agent or trusted environments, practical impact is limited. In Telegram webhook mode, account-level secret wiring could be missed unless an explicit monitor webhook secret override was provided. Version 2026.2.15 fixes the issue.	5.5	More Details
CVE-2026-27117	bit7z is a cross-platform C++ static library that allows the compression/extraction of archive files. Prior to version 4.0.11, a path traversal vulnerability ("Zip Slip") exists in bit7z's archive extraction functionality. The library does not adequately validate file paths contained in archive entries, allowing files to be written outside the intended extraction directory through three distinct mechanisms: relative path traversal, absolute path traversal, and symbolic link traversal. An attacker can exploit this by providing a malicious archive to any application that uses bit7z to extract untrusted archives. Successful exploitation results in arbitrary file write with the privileges of the process performing the extraction. This could lead to overwriting of application binaries, configuration files, or other sensitive data. The vulnerability does not directly enable reading of file contents; the confidentiality impact is limited to the calling application's own behavior after extraction. However, applications that	5.5	More Details

	subsequently serve or display extracted files may face secondary confidentiality risks from attacker-created symlinks. Fixes have been released in version 4.0.11. If upgrading is not immediately possible, users can mitigate the vulnerability by validating each entry's destination path before writing. Other mitigations include running extraction with least privilege and extracting untrusted archives in a sandboxed directory.		
CVE-2025-14876	A flaw was found in the virtio-crypto device of QEMU. A malicious guest operating system can exploit a missing length limit in the AKCIPHER path, leading to uncontrolled memory allocation. This can result in a denial of service (DoS) on the host system by causing the QEMU process to terminate unexpectedly.	5.5	More Details
CVE-2026-22568	Improper neutralization of special elements in user-supplied input within the ZIA Admin UI could allow an authenticated administrator to access or retrieve unauthorized internal information in rare conditions.	5.5	More Details
CVE-2026-27003	OpenClaw is a personal AI assistant. Telegram bot tokens can appear in error messages and stack traces (for example, when request URLs include `https://api.telegram.org/bot<token>/...`). Prior to version 2026.2.15, OpenClaw logged these strings without redaction, which could leak the bot token into logs, crash reports, CI output, or support bundles. Disclosure of a Telegram bot token allows an attacker to impersonate the bot and take over Bot API access. Users should upgrade to version 2026.2.15 to obtain a fix and rotate the Telegram bot token if it may have been exposed.	5.5	More Details
CVE-2026-27014	NanaZip is an open source file archive Starting in version 5.0.1252.0 and prior to version 6.0.1630.0, circular `NextOffset` chains cause an infinite loop, and deeply nested directories cause unbounded recursion (stack overflow) in the ROMFS archive parser. Version 6.0.1630.0 patches the issue.	5.5	More Details
CVE-2026-25385	Server-Side Request Forgery (SSRF) vulnerability in KaizenCoders URL Shortify url-shortify allows Server Side Request Forgery.This issue affects URL Shortify: from n/a through <= 1.12.3.	5.5	More Details
CVE-2026-27026	pypdf is a free and open-source pure-python PDF library. Prior to 6.7.1, an attacker who uses this vulnerability can craft a PDF which leads to long runtimes. This requires a malformed /FlateDecode stream, where the byte-by-byte decompression is used. This vulnerability is fixed in 6.7.1.	5.5	More Details
CVE-2026-2898	A vulnerability was detected in funadmin up to 7.1.0-rc4. This issue affects the function getMember of the file app/common/service/AuthCloudService.php of the component Backend Endpoint. The manipulation of the argument cloud_account results in deserialization. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2025-61143	libtiff up to v4.7.1 was discovered to contain a NULL pointer dereference via the component libtiff/tif_open.c.	5.5	More Details
CVE-2026-27024	pypdf is a free and open-source pure-python PDF library. Prior to 6.7.1, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires accessing the children of a TreeObject, for example as part of outlines. This vulnerability is fixed in 6.7.1.	5.5	More Details
CVE-2026-27025	pypdf is a free and open-source pure-python PDF library. Prior to 6.7.1, an attacker who uses this vulnerability can craft a PDF which leads to long runtimes and large memory consumption. This requires parsing the /ToUnicode entry of a font with unusually large values, for example during text extraction. This vulnerability is fixed in 6.7.1.	5.5	More Details
CVE-2026-25388	Missing Authorization vulnerability in scripteo Ads Pro ap-plugin-scripteo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ads Pro: from n/a through <= 5.0.	5.4	More Details
CVE-2026-27742	Bludit version 3.16.2 contains a stored cross-site scripting (XSS) vulnerability in the post content functionality. The application performs client-side sanitation of content input but does not enforce equivalent sanitation on the server side. An authenticated user can inject arbitrary JavaScript into the content field of a post, which is stored and later rendered to other users without proper output encoding. When viewed, the injected script executes in the context of the victim’s browser, allowing session hijacking, credential theft, content manipulation, or other actions within the user’s privileges.	5.4	More Details
CVE-2026-23618	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Spam Keyword Checking (Subject) conditions interface. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pvSubject$TXB_SubjectCondition parameter to /MailEssentials/pages/MailSecurity/ASKeywordChecking.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-25322	Cross-Site Request Forgery (CSRF) vulnerability in PublishPress PublishPress Revisions revisionary allows Cross Site Request Forgery.This issue affects PublishPress Revisions: from n/a through <= 3.7.22.	5.4	More Details
CVE-2026-27122	svelte performance oriented web framework. Prior to 5.51.5, when using <svelte:element this={tag}> in server-side rendering, the provided tag name is not validated or sanitized before being emitted into the HTML output. If the tag string contains unexpected characters, it can result in HTML injection in the SSR output. Client-side rendering is not affected. This vulnerability is fixed in 5.51.5.	5.4	More Details
CVE-2026-26059	ChurchCRM is an open-source church management system. In versions prior to 6.8.2, it was possible for an authenticated user with permission to edit groups to store a JavaScript payload that would execute when the group was viewed in the Group View. Version 6.8.2 fixes this issue.	5.4	More Details
CVE-2026-27121	svelte performance oriented web framework. Versions of svelte prior to 5.51.5 are vulnerable to cross-site scripting (XSS) during server-side rendering. When using spread syntax to render attributes from untrusted data, event handler properties are included in the rendered HTML output. If an application spreads user-controlled or external data as element attributes, an attacker can inject malicious event handlers that execute in victims' browsers. This vulnerability is fixed in 5.51.5.	5.4	More Details
CVE-	svelte performance oriented web framework. From 5.39.3, <=5.51.4, in certain circumstances, the server-side rendering output		

2026-27119	of an <option> element does not properly escape its content, potentially allowing HTML injection in the SSR output. Client-side rendering is not affected. This vulnerability is fixed in 5.51.5.	5.4	More Details
CVE-2026-25311	Missing Authorization vulnerability in 10up Autoshare for Twitter autoshare-for-twitter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Autoshare for Twitter: from n/a through <= 2.3.1.	5.4	More Details
CVE-2026-27474	SPIP before 4.4.9 allows Cross-Site Scripting (XSS) in the private area, complementing an incomplete fix from SPIP 4.4.8. The echappe_anti_xss() function was not systematically applied to input, form, button, and anchor (a) HTML tags, allowing an attacker to inject malicious scripts through these elements. This vulnerability is not mitigated by the SPIP security screen.	5.4	More Details
CVE-2026-27147	GetSimple CMS is a content management system. All versions of GetSimple CMS are vulnerable to XSS through SVG file uploads. Authenticated users can upload SVG files via the administrative upload functionality, but they are not properly sanitized or restricted, allowing an attacker to embed malicious JavaScript. When the uploaded SVG file is accessed, the script executes in the browser. This issue does not have a fix at the time of publication.	5.4	More Details
CVE-2026-23619	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Local Domains settings page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$Pv3$txtDescription parameter to /MailEssentials/pages/MailSecurity/general.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23804	Missing Authorization vulnerability in BBR Plugins Better Business Reviews better-business-reviews allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Better Business Reviews: from n/a through <= 0.1.1.	5.4	More Details
CVE-2025-71240	SPIP before 4.2.15 allows Cross-Site Scripting (XSS) via crafted content in HTML code tags. The application does not properly verify JavaScript within code tags, allowing an attacker to inject malicious scripts that execute in a victim's browser.	5.4	More Details
CVE-2019-25400	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the fwhosts.cgi script that allow attackers to inject malicious scripts through multiple parameters including HOSTNAME, IP, SUBNET, NETREMARK, HOSTREMARK, newhost, grp_name, remark, SRV_NAME, SRV_PORT, SRVGRP_NAME, SRVGRP_REMARK, and updatesrvgrp. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated users' browsers.	5.4	More Details
CVE-2025-71241	SPIP before 4.3.6, 4.2.17, and 4.1.20 allows Cross-Site Scripting (XSS) in the private area. The content of the error message displayed by the 'transmettre' API is not properly sanitized, allowing an attacker to inject malicious scripts. This vulnerability is mitigated by the SPIP security screen.	5.4	More Details
CVE-2026-25391	Missing Authorization vulnerability in WP Grids WP Wand ai-content-generation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Wand: from n/a through <= 1.3.07.	5.4	More Details
CVE-2026-25337	Cross-Site Request Forgery (CSRF) vulnerability in wpcoachify Coachify coachify allows Cross Site Request Forgery.This issue affects Coachify: from n/a through <= 1.1.5.	5.4	More Details
CVE-2026-23617	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Spam Keyword Checking (Body) conditions interface. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pvGeneral$TXB_Condition parameter to /MailEssentials/pages/MailSecurity/ASKeywordChecking.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-25500	Rack is a modular Ruby web server interface. Prior to versions 2.2.22, 3.1.20, and 3.2.5, `Rack::Directory` generates an HTML directory index where each file entry is rendered as a clickable link. If a file exists on disk whose basename starts with the `javascript:` scheme (e.g. `javascript:alert(1)`), the generated index contains an anchor whose `href` is exactly `javascript:alert(1)`. Clicking the entry executes JavaScript in the browser (demonstrated with `alert(1)`). Versions 2.2.22, 3.1.20, and 3.2.5 fix the issue.	5.4	More Details
CVE-2026-2863	A flaw has been found in feng_ha_ha/megagao ssm-erp and production_ssm up to 4288d53bd35757b27f2d070057aefb2c07bdd097. The impacted element is the function deleteFile of the file FileServiceImpl.java. This manipulation causes path traversal. 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. This product is distributed under two entirely different names. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-27387	Missing Authorization vulnerability in designinvento DirectoryPress directorypress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DirectoryPress: from n/a through <= 3.6.26.	5.4	More Details
CVE-2026-23605	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Attachment Filtering rule creation workflow. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$TXB_RuleName parameter to /MailEssentials/pages/MailSecurity/attachmentchecking.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23604	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Keyword Filtering rule creation workflow. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$TXB_RuleName parameter to /MailEssentials/pages/MailSecurity/contentchecking.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
	A vulnerability has been found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. Affected by this issue is the function deleteCache/removeAllCache/syncCache of the file		

CVE-2026-2849	dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\CacheController.java of the component Cache Sync Handler. Such manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-22341	Authentication Bypass Using an Alternate Path or Channel vulnerability in Case-Themes Booked booked allows Authentication Abuse.This issue affects Booked: from n/a through <= 3.0.0.	5.4	More Details
CVE-2026-2953	A vulnerability has been found in Dromara UJCMS 101.2. This issue affects the function deleteDirectory of the file WebFileTemplateController.delete of the component Template Handler. Such manipulation leads to path traversal. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-26345	SPIP before 4.4.8 contains a stored cross-site scripting (XSS) vulnerability in the public area triggered in certain edge-case usage patterns. The echapper_html_suspect() function does not adequately sanitize user-controlled content, allowing authenticated users with content-editing privileges (e.g., author-level roles and above) to inject malicious scripts. The injected payload may be rendered across multiple pages within the framework and execute in the browser context of other users, including administrators. Successful exploitation can allow attackers to perform actions in the security context of the victim user, including unauthorized modification of application state. This vulnerability is not mitigated by the SPIP security screen.	5.4	More Details
CVE-2026-26223	SPIP before 4.4.8 allows cross-site scripting (XSS) in the private area via malicious iframe tags. The application does not properly sandbox or escape iframe content in the back-office, allowing an attacker to inject and execute malicious scripts. The fix adds a sandbox attribute to iframe tags in the private area. This vulnerability is not mitigated by the SPIP security screen.	5.4	More Details
CVE-2026-27050	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress RealPress realpress allows Cross Site Request Forgery.This issue affects RealPress: from n/a through <= 1.1.0.	5.4	More Details
CVE-2026-2957	A weakness has been identified in qinming99 dst-admin up to 1.5.0. This impacts the function deleteBackup of the file src/main/java/com/tugos/dst/admin/controller/BackupController.java of the component File Handler. This manipulation causes denial of service. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-23858	Dell Wyse Management Suite, versions prior to WMS 5.5, contain an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Script Injection.	5.4	More Details
CVE-2026-27016	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 24.10.0 through 26.1.1 are vulnerable to Stored XSS via the unit parameter in Custom OID. The Custom OID functionality lacks strip_tags() sanitization while other fields (name, oid, datatype) are sanitized. The unsanitized value is stored in the database and rendered without HTML escaping. This issue is fixed in version 26.2.0.	5.4	More Details
CVE-2026-2997	Tronclass developed by WisdomGarden has a Insecure Direct Object Reference vulnerability. After obtaining a course ID, authenticated remote attackers to modify a specific parameter to obtain a course invitation code, thereby joining any course.	5.4	More Details
CVE-2026-26952	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. Versions 6.4 and below are vulnerable to stored HTML injection through the local DNS records configuration page, which allows an authenticated administrator to inject code that is stored in the Pi-hole configuration and rendered every time the DNS records table is viewed. The populateDataTable() function contains a data variable with the full DNS record value exactly as entered by the user and returned by the API. This value is inserted directly into the data-tag HTML attribute without any escaping or sanitization of special characters. When an attacker supplies a value containing double quotes ("), they can prematurely “close” the data-tag attribute and inject additional HTML attributes into the element. Since Pi-hole implements a Content Security Policy (CSP) that blocks inline JavaScript, the impact is limited. This issue has been fixed in version 6.4.1.	5.4	More Details
CVE-2025-15582	A security flaw has been discovered in detronetdip E-commerce 1.0.0. The impacted element is the function Delete/Update of the component Product Management Module. Performing a manipulation of the argument ID results in authorization bypass. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-25739	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Versions prior to 3.3.10 are vulnerable to cross-site scripting when uploading certain file types as materials. Users should upgrade to version 3.3.10 to receive a patch. To apply the fix itself updating is sufficient, but to benefit from the strict Content Security Policy (CSP) Indico now applies by default for file downloads, update the webserver config in case one uses nginx with Indico's `STATIC_FILE_METHOD` set to `xaccelredirect`. For further directions, consult the GitHub Security advisory or Indico setup documentation. Some workarounds are available. Use the webserver config to apply a strict CSP for material download endpoints, and/or only let trustworthy users create content (including material uploads, which speakers can typically do as well) on Indico.	5.4	More Details
CVE-2026-26953	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. Versions 6.0 and above have a Stored HTML Injection vulnerability in the active sessions table located on the API settings page, allowing an attacker with valid credentials to inject arbitrary HTML code that will be rendered in the browser of any administrator who visits the active sessions page. The rowCallback function contains the value data.x_forwarded_for, which is directly concatenated into an HTML string and inserted into the DOM using jQuery’s .html() method. This method interprets the content as HTML, which means that any HTML tags present in the value will be parsed and rendered by the browser. An attacker can use common tools such as curl, wget, Python requests, Burp Suite, or even JavaScript fetch() to send an authentication request with an X-Forwarded-For header that contains malicious HTML code instead of a legitimate IP address. Since Pi-hole implements a Content Security Policy (CSP) that blocks inline JavaScript, the impact is limited to pure HTML injection without the ability to execute scripts. This issue has been fixed in version 6.4.1.	5.4	More Details

CVE-2026-2735	Stored Cross-Site Scripting (XSS) in Alkacon's OpenCms v18.0, which occurs when user input is not properly validated when sending a POST request to '/blog/new-article/org.opencms.ugc.CmsUgcEditService.gwt' using the 'text' parameter.	5.4	More Details
CVE-2026-23606	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Advanced Content Filtering rule creation workflow. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$txtRuleName parameter to /MailEssentials/pages/MailSecurity/advancedfiltering.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-27517	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior reflect unsanitized user input in the web interface, allowing an attacker to inject and execute arbitrary JavaScript in the context of an authenticated user.	5.4	More Details
CVE-2026-25473	Missing Authorization vulnerability in AA-Team WZone woozone allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WZone: from n/a through <= 14.0.31.	5.4	More Details
CVE-2026-2284	The News Element Elementor Blog Magazine plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.8. This is due to a missing capability check and nonce verification on the 'ne_clean_data' AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to truncate 8 core WordPress database tables (posts, comments, terms, term_relationships, term_taxonomy, postmeta, commentmeta, termmeta) and delete the entire WordPress uploads directory, resulting in complete data loss.	5.4	More Details
CVE-2026-27458	LinkAce is a self-hosted archive to collect website links. Versions 2.4.2 and below have a Stored Cross-site Scripting vulnerability through the Atom feed endpoint for lists (/lists/feed). An authenticated user can inject a CDATA-breaking payload into a list description that escapes the XML CDATA section, injects a native SVG element into the Atom XML document, and executes arbitrary JavaScript directly in the browser when the feed URL is visited. No RSS reader or additional rendering context is required — the browser's native XML parser processes the injected SVG and fires the onload event handler. This vulnerability exists because the lists feed template outputs list descriptions using Blade's raw syntax ({!! !!}) without sanitization inside a CDATA block. The critical detail is that because the output sits inside <![CDATA[...]]>, an attacker can inject the sequence]]> to close the CDATA section prematurely, then inject arbitrary XML/SVG elements that the browser parses and executes natively as part of the Atom document. This issue has been fixed in version 2.4.3.	5.4	More Details
CVE-2026-23616	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Anti-Spoofing configuration page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$AntiSpoofingGeneral1$TxtSmtpDesc parameter to /MailEssentials/pages/MailSecurity/AntiSpoofing.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-2804	Use-after-free in the JavaScript: WebAssembly component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	5.4	More Details
CVE-2026-2864	A vulnerability has been found in feng_ha_ha/megagao ssm-erp and production_ssm up to 4288d53bd35757b27f2d070057aefb2c07bdd097. This affects the function pictureDelete of the file PictureController.java. Such manipulation of the argument picName leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. This product is distributed under two entirely different names. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-2127	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to unauthorized arbitrary shortcode execution in all versions up to, and including, 1.70.4. This is due to a missing capability check on the `siteorigin_widget_preview_widget_action()` function which is registered via the `wp_ajax_so_widgets_preview` AJAX action. The function only verifies a nonce (`widgets_action`) but does not check user capabilities. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes by invoking the `SiteOrigin_Widget_Editor_Widget` via the preview endpoint. The required nonce is exposed on the public frontend when the Post Carousel widget is present on a page, embedded in the `data-ajax-url` HTML attribute.	5.4	More Details
CVE-2026-23615	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Sender Policy Framework Email Exceptions interface. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv4$txtEmailDescription parameter to /MailEssentials/pages/MailSecurity/SenderPolicyFramework.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23614	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Sender Policy Framework IP Exceptions interface. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv2$txtIPDescription parameter to /MailEssentials/pages/MailSecurity/SenderPolicyFramework.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23607	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Anti-Spam Whitelist management interface. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$txtDescription parameter to /MailEssentials/pages/MailSecurity/Whitelist.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23612	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the IP DNS Blocklist configuration page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$TXB_IPs parameter to /MailEssentials/pages/MailSecurity/ipdnsblocklist.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the IP Blocklist management page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$txtIPDescription parameter to /MailEssentials/pages/MailSecurity/ipblocklist.aspx, which is stored and later rendered in the management interface, allowing	5.4	More Details

23611	script execution in the context of a logged-in user.		
CVE-2026-23613	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the URI DNS Blocklist configuration page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv1$TXB_URIs parameter to /MailEssentials/pages/MailSecurity/uridnsblocklist.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-26270	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane (latest version) that allows an authenticated user with permissions to manage Invoice Groups to inject malicious JavaScript into the "Identifier Format" field. This script executes when any user views the invoice list or the main dashboard. Version 1.7.1 patches the issue.	5.4	More Details
CVE-2026-23609	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Perimeter SMTP Servers configuration page. An authenticated user can supply HTML/JavaScript in the ctl00$ContentPlaceHolder1$pv3$txtDescription parameter to /MailEssentials/pages/MailSecurity/PerimeterSMTPServers.aspx, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-23608	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the Mail Monitoring rule creation endpoint. An authenticated user can supply HTML/JavaScript in the JSON \"name\" field to /MailEssentials/pages/MailSecurity/MailMonitoring.aspx/Save, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2025-69287	The BSV Blockchain SDK is a unified TypeScript SDK for developing scalable apps on the BSV Blockchain. Prior to version 2.0.0, a cryptographic vulnerability in the TypeScript SDK's BRC-104 authentication implementation caused incorrect signature data preparation, resulting in signature incompatibility between SDK implementations and potential authentication bypass scenarios. The vulnerability was located in the `Peer.ts` file of the TypeScript SDK, specifically in the `processInitialRequest` and `processInitialResponse` methods where signature data is prepared for BRC-104 mutual authentication. The TypeScript SDK incorrectly prepared signature data by concatenating base64-encoded nonce strings (`message.initialNonce + sessionNonce`) then decoding the concatenated base64 string (`base64ToBytes(concatenatedString)`). This produced ~32-34 bytes of signature data instead of the correct 64 bytes. BRC-104 authentication relies on cryptographic signatures to establish mutual trust between peers. When signature data preparation is incorrect, signatures generated by the TypeScript SDK don't match those expected by Go/Python SDKs; cross-implementation authentication fails; and an attacker could potentially exploit this to bypass authentication checks. The fix in version 2.0.0 ensures all SDKs now produce identical cryptographic signatures, restoring proper mutual authentication across implementations.	5.4	More Details
CVE-2026-23610	GFI MailEssentials AI versions prior to 22.4 contain a stored cross-site scripting vulnerability in the POP2Exchange configuration endpoint. An authenticated user can supply HTML/JavaScript in the POP3 server login field within the JSON \"popServers\" payload to /MailEssentials/pages/MailSecurity/POP2Exchange.aspx/Save, which is stored and later rendered in the management interface, allowing script execution in the context of a logged-in user.	5.4	More Details
CVE-2026-22422	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in wpeverest Everest Forms everest-forms allows Code Injection.This issue affects Everest Forms: from n/a through <= 3.4.1.	5.3	More Details
CVE-2025-7630	Improper Restriction of Excessive Authentication Attempts, Improper Authentication vulnerability in Doruk Communication and Automation Industry and Trade Inc. Wispotter allows Password Brute Forcing, Brute Force.This issue affects Wispotter: from 1.0 before v2025.10.08.1.	5.3	More Details
CVE-2026-25005	Authorization Bypass Through User-Controlled Key vulnerability in N-Media Frontend File Manager nmedia-user-file-uploader allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Frontend File Manager: from n/a through <= 23.5.	5.3	More Details
CVE-2025-13079	The Popup Builder – Create highly converting, mobile friendly marketing popups. plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.4.2. This is due to the plugin generating predictable unsubscribe tokens using deterministic data. This makes it possible for unauthenticated attackers to unsubscribe arbitrary subscribers from mailing lists via brute-forcing the unsubscribe token, granted they know the victim's email address	5.3	More Details
CVE-2025-13842	The Breadcrumb NavXT plugin for WordPress is vulnerable to authorization bypass through user-controlled key in versions up to and including 7.5.0. This is due to the Gutenberg block renderer trusting the $_REQUEST['post_id'] parameter without verification in the includes/blocks/build/breadcrumb-trail/render.php file. This makes it possible for unauthenticated attackers to enumerate and view breadcrumb trails for draft or private posts by manipulating the post_id parameter, revealing post titles and hierarchy that should remain hidden.	5.3	More Details
CVE-2025-13864	The Breeze - WordPress Cache Plugin plugin for WordPress is vulnerable to unauthorized cache clearing in all versions up to, and including, 2.2.21. This is due to the REST API endpoint `/wp-json/breeze/v1/clear-all-cache` being registered with `permission_callback => '__return_true'` and authentication being disabled by default when the API is enabled. This makes it possible for unauthenticated attackers to clear all site caches (page cache, Varnish, and Cloudflare) via a simple POST request, granted the administrator has enabled the API integration feature.	5.3	More Details
CVE-2025-13930	The Checkout Field Manager (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 7.8.5. This is due to the plugin not properly verifying that a user is authorized to delete an attachment combined with flawed guest order ownership validation. This makes it possible for unauthenticated attackers to delete attachments associated with guest orders using only the publicly available wooccm_upload nonce and attachment ID.	5.3	More Details
CVE-2026-25000	Missing Authorization vulnerability in Kraft Plugins Wheel of Life wheel-of-life allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wheel of Life: from n/a through <= 1.2.0.	5.3	More Details
CVE-2026-	A flaw was found in the blst cryptographic library. This out-of-bounds stack write vulnerability, specifically in the blst_sha256_bcopy assembly routine, occurs due to a missing zero-length guard. A remote attacker can exploit this by providing a zero-length salt parameter to key generation functions, such as blst_keygen_v5(), if the application exposes this	5.3	More Details

2681	functionality. Successful exploitation leads to memory corruption and immediate process termination, resulting in a denial-of-service (DoS) condition.		
CVE-2025-12500	The Checkout Field Manager (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to unauthenticated limited file upload in all versions up to, and including, 7.8.1. This is due to the plugin not properly verifying that a user is authorized to perform file upload actions via the "ajax_checkout_attachment_upload" function. This makes it possible for unauthenticated attackers to upload files to the server, though file types are limited to WordPress's default allowed MIME types (images, documents, etc.).	5.3	More Details
CVE-2026-24999	Missing Authorization vulnerability in Alma Alma alma-gateway-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Alma: from n/a through <= 5.16.1.	5.3	More Details
CVE-2026-2126	The User Submitted Posts – Enable Users to Submit Posts from the Front End plugin for WordPress is vulnerable to Incorrect Authorization in all versions up to, and including, 20260113. This is due to the `usp_get_submitted_category()` function accepting user-submitted category IDs from the POST body without validating them against the admin-configured allowed categories stored in `usp_options['categories']`. This makes it possible for unauthenticated attackers to assign submitted posts to arbitrary categories, including restricted ones, by crafting a direct POST request with manipulated `user-submitted-category[]` values, bypassing the frontend category restrictions.	5.3	More Details
CVE-2026-24375	Missing Authorization vulnerability in WP Swings Ultimate Gift Cards For WooCommerce woo-gift-cards-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Gift Cards For WooCommerce: from n/a through <= 3.2.4.	5.3	More Details
CVE-2025-14294	The Razorpay for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the getCouponList() function in all versions up to, and including, 4.7.8. This is due to the checkAuthCredentials() permission callback always returning true, providing no actual authentication. This makes it possible for unauthenticated attackers to modify the billing and shipping contact information (email and phone) of any WooCommerce order by knowing or guessing the order ID.	5.3	More Details
CVE-2025-13113	The Web Accessibility by accessiBe plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.11. This is due to the `accessibe_render_js_in_footer()` function logging the complete plugin options array to the browser console on public pages, without restricting output to privileged users or checking for debug mode. This makes it possible for unauthenticated attackers to view sensitive configuration data, including email addresses, accessiBe user IDs, account IDs, and license information, via the browser console when the widget is disabled.	5.3	More Details
CVE-2026-26745	OpenSourcePOS 3.4.1 has a second order SQL Injection vulnerability in the handling of the currency_symbol configuration field. Although the input is initially stored without immediate execution, it is later concatenated into a dynamically constructed SQL query without proper sanitization or parameter binding. This allows an attacker with access to modify the currency_symbol value to inject arbitrary SQL expressions, which are executed when the affected query is subsequently processed.	5.3	More Details
CVE-2026-2653	A security flaw has been discovered in admesh up to 0.98.5. This issue affects the function stl_check_normal_vector of the file src/normals.c. Performing a manipulation results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. It looks like this product is not really maintained anymore.	5.3	More Details
CVE-2025-14357	The Mega Store Woocommerce theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the setup_widgets() function in core/includes/importer/whizzie.php in all versions up to, and including, 5.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary pages and modify site settings.	5.3	More Details
CVE-2025-14444	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to payment bypass due to insufficient verification of data authenticity on the 'process_paypal_sdk_payment' function in all versions up to, and including, 6.0.6.9. This is due to the plugin trusting client-supplied values for payment verification without validating that the payment actually went through PayPal. This makes it possible for unauthenticated attackers to bypass paid registration by manipulating payment status and activating their account without completing a real PayPal payment.	5.3	More Details
CVE-2026-25766	Echo is a Go web framework. In versions 5.0.0 through 5.0.2 on Windows, Echo's `middleware.Static` using the default filesystem allows path traversal via backslashes, enabling unauthenticated remote file read outside the static root. In `middleware/static.go`, the requested path is unescaped and normalized with `path.Clean` (URL semantics). `path.Clean` does not treat `\` as a path separator, so `..\` sequences remain in the cleaned path. The resulting path is then passed to `currentFS.Open(...)`. When the filesystem is left at the default (nil), Echo uses `defaultFS` which calls `os.Open` (`echo.go:792`). On Windows, `os.Open` treats `\` as a path separator and resolves `..\`, allowing traversal outside the static root. Version 5.0.3 fixes the issue.	5.3	More Details
CVE-2026-1219	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions 4.0 to 5.10 via the 'load_track_note_ajax' due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to view the contents of private posts.	5.3	More Details
CVE-2026-25415	Missing Authorization vulnerability in iqonicdesign WPBookit Pro wpbookit-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPBookit Pro: from n/a through <= 1.6.18.	5.3	More Details
CVE-2026-25970	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a signed integer overflow vulnerability in ImageMagick's SIXEL decoder allows an attacker to trigger memory corruption and denial of service when processing a maliciously crafted SIXEL image file. The vulnerability occurs during buffer reallocation operations where pointer arithmetic using signed 32-bit integers overflows. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-	This affects versions of the package bn.js before 5.2.3. Calling maskn(0) on any BN instance corrupts the internal state, causing		More

2026-2739	toString(), divmod(), and other methods to enter an infinite loop, hanging the process indefinitely.	5.3	Details
CVE-2026-27042	Missing Authorization vulnerability in WPDeveloper NotificationX notificationx allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects NotificationX: from n/a through <= 3.2.1.	5.3	More Details
CVE-2026-1938	The YayMail – WooCommerce Email Customizer plugin for WordPress is vulnerable to unauthorized license key deletion due to a missing authorization check on the `/yaymail-license/v1/license/delete` REST endpoint in versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to delete the plugin's license key via the '/yaymail-license/v1/license/delete' endpoint granted they can obtain the REST API nonce.	5.3	More Details
CVE-2026-2385	The The Plus Addons for Elementor – Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in all versions up to, and including, 6.4.7. This is due to the plugin decrypting and trusting attacker-controlled email_data in an unauthenticated AJAX handler without cryptographic authenticity guarantees. This makes it possible for unauthenticated attackers to tamper with form email routing and redirection values to trigger unauthorized email relay and attacker-controlled redirection via the 'email_data' parameter.	5.3	More Details
CVE-2025-12074	The Context Blog theme for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.5 via the 'context_blog_modal_popup' due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	5.3	More Details
CVE-2026-25969	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-15, a memory leak exists in `coders/ashlar.c`. The `WriteASHLARImage` allocates a structure. However, when an exception is thrown, the allocated memory is not properly released, resulting in a potential memory leak. Version 7.1.2-15 contains a patch.	5.3	More Details
CVE-2026-25983	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a crafted MSL script triggers a heap-use-after-free. The operation element handler replaces and frees the image while the parser continues reading from it, leading to a UAF in ReadBlobString during further parsing. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25408	Missing Authorization vulnerability in PluginRx Broken Link Notifier broken-link-notifier allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Broken Link Notifier: from n/a through <= 1.3.5.	5.3	More Details
CVE-2026-25986	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap buffer overflow write vulnerability exists in ReadYUVImage() (coders/yuv.c) when processing malicious YUV 4:2:2 (NoInterlace) images. The pixel-pair loop writes one pixel beyond the allocated row buffer. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-27328	Missing Authorization vulnerability in DevsBlink EduBlink edublink allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EduBlink: from n/a through <= 2.0.7.	5.3	More Details
CVE-2026-2894	A vulnerability was identified in funadmin up to 7.1.0-rc4. Affected by this vulnerability is the function getMember of the file app/frontend/view/login/forget.html. Such manipulation leads to information disclosure. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-67970	Missing Authorization vulnerability in vertim Schedula schedula-smart-appointment-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Schedula: from n/a through <= 1.0.	5.3	More Details
CVE-2026-25441	Missing Authorization vulnerability in LeadConnector LeadConnector leadconnector allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LeadConnector: from n/a through <= 3.0.21.	5.3	More Details
CVE-2026-25527	changedetection.io is a free open source web page change detection tool. In versions prior to 0.53.2, the `/static/<group>/<filename>` route accepts `group=".."`, which causes `send_from_directory("static/..", filename)` to execute. This moves the base directory up to `/app/changedetectionio`, enabling unauthenticated local file read of application source files (e.g., `flask_app.py`). Version 0.53.2 fixes the issue.	5.3	More Details
CVE-2026-26744	A user enumeration vulnerability exists in FormaLMS 4.1.18 and below in the password recovery functionality accessible via the /lostpwd endpoint. The application returns different error messages for valid and invalid usernames allowing an unauthenticated attacker to determine which usernames are registered in the system through observable response discrepancy.	5.3	More Details
CVE-2026-25799	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a logic error in YUV sampling factor validation allows an invalid sampling factor to bypass checks and trigger a division-by-zero during image loading, resulting in a reliable denial-of-service. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25798	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a NULL pointer dereference in ClonePixelCacheRepository allows a remote attacker to crash any application linked against ImageMagick by supplying a crafted image file, resulting in denial of service. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25796	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, in `ReadSTEGANOImage()` (`coders/stegano.c`), the `watermark` Image object is not freed on three early-return paths, resulting in a definite memory leak (~13.5KB+ per invocation) that can be exploited for denial of service. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and		

CVE-2026-25795	6.9.13-40, in `ReadSFWImage()` (`coders/sfw.c`), when temporary file creation fails, `read_info` is destroyed before its `filename` member is accessed, causing a NULL pointer dereference and crash. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-27017	uTLS is a fork of crypto/tls, created to customize ClientHello for fingerprinting resistance while still using it for the handshake. Versions 1.6.0 through 1.8.0 contain a fingerprint mismatch with Chrome when using GREASE ECH, related to cipher suite selection. When Chrome selects the preferred cipher suite in the outer ClientHello and for ECH, it does so consistently based on hardware support—for example, if it prefers AES for the outer cipher suite, it also uses AES for ECH. However, the Chrome parrot in uTLS hardcodes AES preference for outer cipher suites but selects the ECH cipher suite randomly between AES and ChaCha20. This creates a 50% chance of selecting ChaCha20 for ECH while using AES for the outer cipher suite, a combination impossible in Chrome. This issue only affects GREASE ECH; in real ECH, Chrome selects the first valid cipher suite when AES is preferred, which uTLS handles correctly. This issue has been fixed in version 1.8.1.	5.3	More Details
CVE-2025-8055	Server-Side Request Forgery (SSRF) vulnerability in OpenText™ XM Fax allows Server Side Request Forgery. The vulnerability could allow an attacker to perform blind SSRF to other systems accessible from the XM Fax server. This issue affects XM Fax: 24.2.	5.3	More Details
CVE-2026-25638	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, memory leak exists in `coders/msl.c`. In the `WriteMSLImage` function of the `msl.c` file, resources are allocated. But the function returns early without releasing these allocated resources. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25637	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-15, a memory leak in the ASHLAR image writer allows an attacker to exhaust process memory by providing a crafted image that results in small objects that are allocated but never freed. Version 7.1.2-15 contains a patch.	5.3	More Details
CVE-2026-26977	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. In versions 2.44.0 and below, unauthorized users are able to access the details of unpublished courses via API endpoints. A fix for this issue is planned for the 2.45.0 release.	5.3	More Details
CVE-2025-15563	Any unauthenticated user can reset the WorkTime on-prem database configuration by sending a specific HTTP request to the WorkTime server. No authorization check is applied here.	5.3	More Details
CVE-2026-27066	Missing Authorization vulnerability in PI Web Solution Live sales notification for WooCommerce live-sales-notifications-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Live sales notification for WooCommerce: from n/a through <= 2.3.46.	5.3	More Details
CVE-2026-26967	PJSIP is a free and open source multimedia communication library written in C. In versions 2.16 and below, there is a critical Heap-based Buffer Overflow vulnerability in PJSIP's H.264 unpacketizer. The bug occurs when processing malformed SRTP packets, where the unpacketizer reads a 2-byte NAL unit size field without validating that both bytes are within the payload buffer bounds. The vulnerability affects applications that receive video using H.264. A patch is available at https://github.com/pjsip/pjproject/commit/f821c214e52b11bae11e4cd3c7f0864538fb5491.	5.3	More Details
CVE-2026-2975	A security flaw has been discovered in FastApiAdmin up to 2.2.0. Affected by this vulnerability is the function reset_api_docs of the file /backend/app/plugin/init_app.py of the component Custom Documentation Endpoint. The manipulation results in information disclosure. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	5.3	More Details
CVE-2026-2605	Tanium addressed an insertion of sensitive information into log file vulnerability in TanOS.	5.3	More Details
CVE-2026-24484	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, Magick fails to check for multi-layer nested mvg conversions to svg, leading to DoS. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-1656	The Business Directory Plugin for WordPress is vulnerable to authorization bypass due to a missing authorization check in all versions up to, and including, 6.4.20. This makes it possible for unauthenticated attackers to modify arbitrary listings, including changing titles, content, and email addresses, by directly referencing the listing ID in crafted requests to the wpbdp_ajax AJAX action.	5.3	More Details
CVE-2025-10256	A NULL pointer dereference vulnerability exists in FFmpeg's Firequalizer filter (libavfilter/af_firequalizer.c) due to a missing check on the return value of av_malloc_array() in the config_input() function. An attacker could exploit this by tricking a victim into processing a crafted media file with the Firequalizer filter enabled, causing the application to dereference a NULL pointer and crash, leading to denial of service.	5.3	More Details
CVE-2026-25384	Missing Authorization vulnerability in WP Lab WP-Lister Lite for eBay wp-lister-for-ebay allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-Lister Lite for eBay: from n/a through <= 3.8.5.	5.3	More Details
CVE-2026-25374	Missing Authorization vulnerability in raratheme Spa and Salon spa-and-salon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spa and Salon: from n/a through <= 1.3.2.	5.3	More Details
CVE-2026-26983	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, the MSL interpreter crashes when processing a invalid `<map>` element that causes it to use an image after it has been freed. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25325	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in rtCamp rtMedia for WordPress, BuddyPress and bbPress buddypress-media allows Retrieve Embedded Sensitive Data.This issue affects rtMedia for WordPress, BuddyPress and bbPress: from n/a through <= 4.7.8.	5.3	More Details

CVE-2026-25332	Missing Authorization vulnerability in Fahad Mahmood Endless Posts Navigation endless-posts-navigation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Endless Posts Navigation: from n/a through <= 2.2.9.	5.3	More Details
CVE-2026-25333	Missing Authorization vulnerability in peregrinethemes Shopwell shopwell allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Shopwell: from n/a through <= 1.0.11.	5.3	More Details
CVE-2026-25336	Missing Authorization vulnerability in wpcoachify Coachify coachify allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Coachify: from n/a through <= 1.1.5.	5.3	More Details
CVE-2026-25338	Missing Authorization vulnerability in Ays Pro AI ChatBot with ChatGPT and Content Generator by AYS ays-chatgpt-assistant allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI ChatBot with ChatGPT and Content Generator by AYS: from n/a through <= 2.7.4.	5.3	More Details
CVE-2026-25348	Missing Authorization vulnerability in alttextai Download Alt Text AI alttext-ai allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Download Alt Text AI: from n/a through <= 1.10.15.	5.3	More Details
CVE-2026-25364	Missing Authorization vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.8.	5.3	More Details
CVE-2026-25321	Missing Authorization vulnerability in PSM Plugins SupportCandy supportcandy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SupportCandy: from n/a through <= 3.4.4.	5.3	More Details
CVE-2026-25320	Missing Authorization vulnerability in Cool Plugins Elementor Contact Form DB sb-elementor-contact-form-db allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Elementor Contact Form DB: from n/a through <= 2.1.3.	5.3	More Details
CVE-2026-25367	Missing Authorization vulnerability in NooTheme CitiLights noo-citilights allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CitiLights: from n/a through < 3.7.2.	5.3	More Details
CVE-2025-69325	Path Traversal: '.../...//' vulnerability in primersoftware Primer MyData for Woocommerce primer-mydata allows Path Traversal.This issue affects Primer MyData for Woocommerce: from n/a through <= 4.2.8.	5.3	More Details
CVE-2026-25324	Authorization Bypass Through User-Controlled Key vulnerability in ExpressTech Systems 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 <= 10.3.4.	5.3	More Details
CVE-2026-25988	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, sometimes msl.c fails to update the stack index, so an image is stored in the wrong slot and never freed on error, causing leaks. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-25386	Missing Authorization vulnerability in Elementor Ally pojo-accessibility allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ally: from n/a through <= 4.0.2.	5.3	More Details
CVE-2026-2861	A vulnerability was detected in Foswiki up to 2.1.10. The affected element is an unknown function of the component Changes/Viewfile/Oops. The manipulation results in information disclosure. It is possible to launch the attack remotely. The exploit is now public and may be used. Upgrading to version 2.1.11 is sufficient to fix this issue. The patch is identified as 31aeecb58b64/d8ed86b10e46. Upgrading the affected component is recommended.	5.3	More Details
CVE-2026-25987	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap buffer over-read vulnerability exists in the MAP image decoder when processing crafted MAP files, potentially leading to crashes or unintended memory disclosure during image decoding. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.3	More Details
CVE-2026-2667	A vulnerability has been found in Rongzhitong Visual Integrated Command and Dispatch Platform up to 20260206. The impacted element is an unknown function of the file /dispatch/api?cmd=userinfo. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-27480	Static Web Server (SWS) is a production-ready web server suitable for static web files or assets. In versions 2.1.0 through 2.40.1, a timing-based username enumeration vulnerability in Basic Authentication allows attackers to identify valid users by exploiting early responses for invalid usernames, enabling targeted brute-force or credential-stuffing attacks. SWS checks whether a username exists before verifying the password, causing valid usernames to follow a slower code path (e.g., bcrypt hashing) while invalid usernames receive an immediate 401 response. This timing discrepancy allows attackers to enumerate valid accounts by measuring response-time differences. This issue has been fixed in version 2.41.0.	5.3	More Details
CVE-2026-25404	Missing Authorization vulnerability in Automattic WP Job Manager wp-job-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Manager: from n/a through <= 2.4.0.	5.3	More Details
CVE-2026-27486	OpenClaw is a personal AI assistant. In versions 2026.2.13 and below of the OpenClaw CLI, the process cleanup uses system-wide process enumeration and pattern matching to terminate processes without verifying if they are owned by the current OpenClaw process. On shared hosts, unrelated processes can be terminated if they match the pattern. The CLI runner cleanup helpers can kill processes matched by command-line patterns without validating process ownership. This issue has been fixed in version 2026.2.14.	5.3	More Details

CVE-2026-25315	Missing Authorization vulnerability in hcaptcha hCaptcha for WP hcaptcha-for-forms-and-more allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects hCaptcha for WP: from n/a through <= 4.22.0.	5.3	More Details
CVE-2026-25576	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-15 and 6.9.13-40, a heap buffer over-read vulnerability exists in multiple raw image format handles. The vulnerability occurs when processing images with -extract dimensions larger than -size dimensions, causing out-of-bounds memory reads from a heap-allocated buffer. Versions 7.1.2-15 and 6.9.13-40 contain a patch.	5.1	More Details
CVE-2026-2243	A flaw was found in QEMU. A specially crafted VMDK image could trigger an out-of-bounds read vulnerability, potentially leading to a 12-byte leak of sensitive information or a denial of service condition (DoS).	5.1	More Details
CVE-2026-2964	A vulnerability was identified in higuma web-audio-recorder-js 0.1/0.1.1. Impacted is the function extend in the library lib/WebAudioRecorder.js of the component Dynamic Config Handling. Such manipulation leads to improperly controlled modification of object prototype attributes. It is possible to launch the attack remotely. Attacks of this nature are highly complex. 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.	5.0	More Details
CVE-2025-61145	libtiff up to v4.7.1 was discovered to contain a double free via the component tools/tiffcrop.c.	5.0	More Details
CVE-2026-25310	Server-Side Request Forgery (SSRF) vulnerability in Alobaidi Extend Link extend-link allows Server Side Request Forgery.This issue affects Extend Link: from n/a through <= 2.0.0.	4.9	More Details
CVE-2025-11848	A null pointer dereference vulnerability in the Wake-on-LAN CGI program of the Zyxel VMG3625-T50B firmware version through 5.50(ABPM.9.6)C0 and the Zyxel WX3100-T0 firmware versions through 5.50(ABVL.4.8)C0 could allow an authenticated attacker with administrator privileges to trigger a denial-of-service (DoS) condition by sending a crafted HTTP request.	4.9	More Details
CVE-2025-8781	The Bookster – WordPress Appointment Booking Plugin plugin for WordPress is vulnerable to SQL Injection via the ‘raw’ parameter in all versions up to, and including, 2.1.1 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 Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-0400	A post-authentication Format String vulnerability in SonicOS allows a remote attacker to crash a firewall.	4.9	More Details
CVE-2025-11845	A null pointer dereference vulnerability in the certificate downloader CGI program of the Zyxel VMG3625-T50B firmware versions through 5.50(ABPM.9.6)C0 and the Zyxel WX3100-T0 firmware versions through 5.50(ABVL.4.8)C0 could allow an authenticated attacker with administrator privileges to trigger a denial-of-service (DoS) condition by sending a crafted HTTP request.	4.9	More Details
CVE-2025-11846	A null pointer dereference vulnerability in the account settings CGI program of the Zyxel VMG3625-T50B firmware versions through 5.50(ABPM.9.6)C0 and the Zyxel WX3100-T0 firmware versions through 5.50(ABVL.4.8)C0 could allow an authenticated attacker with administrator privileges to trigger a denial-of-service (DoS) condition by sending a crafted HTTP request.	4.9	More Details
CVE-2025-11847	A null pointer dereference vulnerability in the IP settings CGI program of the Zyxel VMG3625-T50B firmware versions through 5.50(ABPM.9.6)C0 and the Zyxel WX3100-T0 firmware versions through 5.50(ABVL.4.8)C0 could allow an authenticated attacker with administrator privileges to trigger a denial-of-service (DoS) condition by sending a crafted HTTP request.	4.9	More Details
CVE-2026-0402	A post-authentication Out-of-bounds Read vulnerability in SonicOS allows a remote attacker to crash a firewall.	4.9	More Details
CVE-2026-0399	Multiple post-authentication stack-based buffer overflow vulnerabilities in the SonicOS management interface due to improper bounds checking in a API endpoint.	4.9	More Details
CVE-2026-0401	A post-authentication NULL Pointer Dereference vulnerability in SonicOS allows a remote attacker to crash a firewall.	4.9	More Details
CVE-2025-0577	An insufficient entropy vulnerability was found in glibc. The getrandom and arc4random family of functions may return predictable randomness if these functions are called again after the fork, which happens concurrently with a call to any of these functions.	4.8	More Details
CVE-2026-25595	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Invoice Number field. An authenticated administrator can inject malicious JavaScript that executes when any administrator views the affected invoice or visits the dashboard. Version 1.7.1 patches the issue.	4.8	More Details
CVE-2026-25596	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Product Unit Name fields. An authenticated administrator can inject malicious JavaScript that executes when any administrator views an invoice containing a product with the malicious unit. Version 1.7.1 patches the issue.	4.8	More Details
CVE-2026-	The LearnPress Export Import – WordPress extension for LearnPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'delete_migrated_data' function in all versions up to, and including, 4.1.0. This	4.8	More

1787	makes it possible for unauthenticated attackers to delete course that have been migrated from Tutor LMS. The Tutor LMS plugin must be installed and activated in order to exploit the vulnerability.		Details
CVE-2026-25594	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Family Name field. The `family_name` value is rendered without HTML encoding inside the family dropdown on the product form. When an administrator creates a family with a malicious name, the payload executes in the browser of any administrator who visits the product form. Version 1.7.1 patches the issue.	4.8	More Details
CVE-2026-26991	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. In versions 26.1.1 and below, the device group name is not sanitized, allowing attackers with admin privileges to perform Stored Cross-Site Scripting (XSS) attacks. When a user adds a device group, an HTTP POST request is sent to the Request-URI "/device-groups". The name of the newly created device group is stored in the value of the name parameter. After the device group is created, the entry is displayed along with relevant buttons such as Rediscover Devices, Edit, and Delete. This issue has been fixed in version 26.2.0.	4.8	More Details
CVE-2026-26992	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. In versions 26.1.1 and below, the port group name is not sanitized, allowing attackers with admin privileges to perform Stored Cross-Site Scripting (XSS) attacks. When a user adds a port group, an HTTP POST request is sent to the Request-URI "/port-groups". The name of the newly created port group is stored in the value of the name parameter. After the port group is created, the entry is displayed along with relevant buttons such as Edit and Delete. This issue has been fixed in version 26.2.0.	4.8	More Details
CVE-2026-1277	The URL Shortify plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 1.12.1 due to insufficient validation on the 'redirect_to' parameter in the promotional dismissal handler. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites via a crafted link.	4.7	More Details
CVE-2026-27492	Lettermint Node.js SDK is the official Node.js SDK for Lettermint. In versions 1.5.0 and below, email properties (such as to, subject, html, text, and attachments) are not reset between sends when a single client instance is reused across multiple .send() calls. This can cause properties from a previous send to leak into a subsequent one, potentially delivering content or recipient addresses to unintended parties. Applications sending emails to different recipients in sequence — such as transactional flows like password resets or notifications — are affected. This issue has been fixed in version 1.5.1.	4.7	More Details
CVE-2026-25392	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in KaizenCoders Update URLs – Quick and Easy way to search old links and replace them with new links in WordPress update-urls allows Phishing.This issue affects Update URLs – Quick and Easy way to search old links and replace them with new links in WordPress: from n/a through <= 1.4.0.	4.7	More Details
CVE-2026-22266	Dell PowerProtect Data Manager, version(s) prior to 19.22, contain(s) an Improper Verification of Source of a Communication Channel vulnerability in the REST API. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	4.7	More Details
CVE-2026-2969	A flaw has been found in datapizza-labs datapizza-ai 0.0.2. Affected is the function ChatPromptTemplate of the file datapizza-ai-core/datapizza/modules/prompt/prompt.py of the component Jinja2 Template Handler. This manipulation of the argument Prompt causes improper neutralization of special elements used in a template engine. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-2408	Tanium addressed a use-after-free vulnerability in the Cloud Workloads Enforce client extension.	4.7	More Details
CVE-2025-69725	An Open Redirect vulnerability in the go-chi/chi >=5.2.2 RedirectSlashes function allows remote attackers to redirect victim users to malicious websites using the legitimate website domain.	4.7	More Details
CVE-2026-22269	Dell PowerProtect Data Manager, version(s) prior to 19.22, contain(s) an Improper Verification of Source of a Communication Channel vulnerability in the REST API. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	4.7	More Details
CVE-2026-3040	A vulnerability was identified in DrayTek Vigor 300B up to 1.5.1.6. This affects the function cgiGetFile of the file /cgi-bin/mainfunction.cgi/uploadlangs of the component Web Management Interface. The manipulation of the argument File leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor confirms that "300B is EoL, and this is an authenticated vulnerability. We don't plan to fix it." This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2026-2666	A flaw has been found in mingSoft MCMS 6.1.1. The affected element is an unknown function of the file /ms/file/uploadTemplate.do of the component Template Archive Handler. Executing a manipulation of the argument File can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2026-26993	Flare is a Next.js-based, self-hostable file sharing platform that integrates with screenshot tools. Versions 1.7.0 and below allow users to upload files without proper content validation or sanitization. By embedding malicious JavaScript within an SVG (or other active content formats such as HTML or XML), an attacker can achieve script execution in the context of the application's origin when a victim views the file in “raw” mode. This results in a stored Cross-Site Scripting (XSS) vulnerability that can be exploited to exfiltrate user data. This issue has been fixed in version 1.7.1.	4.6	More Details
CVE-2026-2970	A vulnerability has been found in datapizza-labs datapizza-ai 0.0.2. Affected by this vulnerability is the function RedisCache of the file datapizza-ai-cache/redis/datapizza/cache/redis/cache.py. Such manipulation leads to deserialization. The attack requires being on the local network. A high complexity level is associated with this attack. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.6	More Details
CVE-2026-27146	GetSimple CMS is a content management system. All versions of GetSimple CMS do not implement CSRF protection on the administrative file upload endpoint. As a result, an attacker can craft a malicious web page that silently triggers a file upload request from an authenticated victim’s browser. The request is accepted without requiring a CSRF token or origin validation. This allows an attacker to upload arbitrary files to the application without the victim’s knowledge or consent. In order to exploit	4.5	More Details

	this vulnerability, the victim must be authenticated to GetSimple CMS (e.g., admin user), and visit an attacker-controlled webpage. This issue does not have a fix at the time of publication.		
CVE-2025-12037	The WP 404 Auto Redirect to Similar Post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-27485	OpenClaw is a personal AI assistant. In versions 2026.2.17 and below, skills/skill-creator/scripts/package_skill.py (a local helper script used when authors package skills) previously followed symlinks while building .skill archives. If an author runs this script on a crafted local skill directory containing symlinks to files outside the skill root, the resulting archive can include unintended file contents. If exploited, this vulnerability can lead to potential unintentional disclosure of local files from the packaging machine into a generated .skill artifact, but requires local execution of the packaging script on attacker-controlled skill contents. This issue has been fixed in version 2026.2.18.	4.4	More Details
CVE-2026-1943	The YayMail – WooCommerce Email Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 4.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Shop Manager-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1043	The PostmarkApp Email Integrator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in versions up to, and including, 2.4. This is due to insufficient input sanitization and output escaping on the pma_api_key and pma_sender_address parameters. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the settings page.	4.4	More Details
CVE-2026-26281	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A stored cross-site scripting (XSS) vulnerability in the Sumex invoice view allows an authenticated user with client and invoice management privileges to execute arbitrary JavaScript in the browser of any user viewing the invoice. This can lead to session hijacking, data theft, or other malicious actions on behalf of the victim user. Version 1.7.1 patches the issue.	4.4	More Details
CVE-2026-2282	The Slidorion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1055	The TalkJS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.1.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1044	The Tennis Court Bookings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1047	The salavat counter Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'image_url' parameter in all versions up to, and including, 0.9.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2026-25428	Server-Side Request Forgery (SSRF) vulnerability in totalsoft TS Poll poll-wp allows Server Side Request Forgery.This issue affects TS Poll: from n/a through <= 2.5.5.	4.4	More Details
CVE-2026-2817	Use of insecure directory in Spring Data Geode snapshot import extracts archives into predictable, permissive directories under the system temp location. On shared hosts, a local user with basic privileges can access another user’s extracted snapshot contents, leading to unintended exposure of cache data.	4.4	More Details
CVE-2026-1649	The Community Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ce_venue_name' parameter in all versions up to, and including, 1.5.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2026-2716	The Client Testimonial Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Testimonial Heading' setting in all versions up to, and including, 2.0. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-13727	The Video Share VOD – Turnkey Video Site Builder Script plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 2.7.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-	The Private Comment plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Label text' setting in all versions up to, and including, 0.0.4. This is due to insufficient input sanitization and output escaping on the plugin's label text option. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in	4.4	More Details

2281	pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2026-1304	The Membership Plugin – Restrict Content for WordPress is vulnerable to Stored Cross-Site Scripting via multiple invoice settings fields in all versions up to, and including, 3.2.18 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2026-25420	Missing Authorization vulnerability in MailerLite MailerLite official-mailerlite-sign-up-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MailerLite: from n/a through <= 1.7.18.	4.3	More Details
CVE-2026-25319	Cross-Site Request Forgery (CSRF) vulnerability in wpzita Zita Elementor Site Library zita-site-library allows Cross Site Request Forgery.This issue affects Zita Elementor Site Library: from n/a through <= 1.6.6.	4.3	More Details
CVE-2026-25416	Missing Authorization vulnerability in blazethemes News Kit Elementor Addons news-kit-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects News Kit Elementor Addons: from n/a through <= 1.4.2.	4.3	More Details
CVE-2026-25411	Cross-Site Request Forgery (CSRF) vulnerability in themastercut Revision Manager TMC revision-manager-tmc allows Cross Site Request Forgery.This issue affects Revision Manager TMC: from n/a through <= 2.8.22.	4.3	More Details
CVE-2026-2672	A security flaw has been discovered in Tsinghua Unigroup Electronic Archives System 3.2.210802(62532). Affected by this vulnerability is the function Download of the file /Search/Subject/downLoad. Performing a manipulation of the argument path results in path traversal. 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.	4.3	More Details
CVE-2026-25410	Missing Authorization vulnerability in tstephenson WP-CORS wp-cors allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-CORS: from n/a through <= 0.2.2.	4.3	More Details
CVE-2026-25409	Missing Authorization vulnerability in crgeary JAMstack Deployments wp-jamstack-deployments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JAMstack Deployments: from n/a through <= 1.1.1.	4.3	More Details
CVE-2026-25330	Missing Authorization vulnerability in PublishPress PublishPress Authors publishpress-authors allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PublishPress Authors: from n/a through <= 4.10.1.	4.3	More Details
CVE-2026-25407	Missing Authorization vulnerability in cookiebot Cookiebot cookiebot allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cookiebot: from n/a through <= 4.6.4.	4.3	More Details
CVE-2026-25393	Missing Authorization vulnerability in sparklewpthemes Hello FSE hello-fse allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hello FSE: from n/a through <= 1.0.6.	4.3	More Details
CVE-2026-27484	OpenClaw is a personal AI assistant. In versions 2026.2.17 and below, the Discord moderation action handling (timeout, kick, ban) uses sender identity from request parameters in tool-driven flows, instead of trusted runtime sender context. In setups where Discord moderation actions are enabled and the bot has the necessary guild permissions, a non-admin user can request moderation actions by spoofing sender identity fields. This issue has been fixed in version 2026.2.18.	4.3	More Details
CVE-2026-2023	The WP Plugin Info Card plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.2.0. This is due to missing nonce validation in the ajax_save_custom_plugin() function, which is disabled by prefixing the check with 'false &&'. This makes it possible for unauthenticated attackers to create or modify custom plugin entries via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-25394	Missing Authorization vulnerability in sparklewpthemes Fitness FSE fitness-fse allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fitness FSE: from n/a through <= 1.0.6.	4.3	More Details
CVE-2026-25402	Missing Authorization vulnerability in echoplugins Knowledge Base for Documentation, FAQs with AI Assistance echo-knowledge-base allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Knowledge Base for Documentation, FAQs with AI Assistance: from n/a through <= 16.011.0.	4.3	More Details
CVE-2026-25399	Missing Authorization vulnerability in CryoutCreations Serious Slider cryout-serious-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Serious Slider: from n/a through <= 1.2.7.	4.3	More Details
CVE-2026-25335	Missing Authorization vulnerability in Ays Pro Secure Copy Content Protection and Content Locking secure-copy-content-protection allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Secure Copy Content Protection and Content Locking: from n/a through <= 5.0.0.	4.3	More Details
CVE-2026-1857	The Gutenberg Blocks with AI by Kadence WP plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.6.1. This is due to insufficient validation of the `endpoint` parameter in the `get_items()` function of the GetResponse REST API handler. The endpoint's permission check only requires `edit_posts` capability (Contributor role) rather than `manage_options` (Administrator). This makes it possible for authenticated attackers, with Contributor-level access and above, to make server-side requests to arbitrary endpoints on the configured GetResponse API server, retrieving sensitive data such as contacts, campaigns, and mailing lists using the site's stored API credentials. The stored API key is also leaked in the request headers.	4.3	More Details

CVE-2026-27205	Flask is a web server gateway interface (WSGI) web application framework. In versions 3.1.2 and below, when the session object is accessed, Flask should set the Vary: Cookie header., resulting in a Use of Cache Containing Sensitive Information vulnerability. The logic instructs caches not to cache the response, as it may contain information specific to a logged in user. This is handled in most cases, but some forms of access such as the Python in operator were overlooked. The severity and risk depend on the application being hosted behind a caching proxy that doesn't ignore responses with cookies, not setting a Cache-Control header to mark pages as private or non-cacheable, and accessing the session in a way that only touches keys without reading values or mutating the session. The issue has been fixed in version 3.1.3.	4.3	More Details
CVE-2026-25395	Missing Authorization vulnerability in ikreatethemes Business Roy business-roy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Business Roy: from n/a through <= 1.1.4.	4.3	More Details
CVE-2026-25375	Missing Authorization vulnerability in WP Chill Image Photo Gallery Final Tiles Grid final-tiles-grid-gallery-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Photo Gallery Final Tiles Grid: from n/a through <= 3.6.10.	4.3	More Details
CVE-2026-2658	A vulnerability was found in newbee-ltd newbee-mall up to a069069b07027613bf0e7f571736be86f431faee. Affected is an unknown function of the component Multiple Endpoints. Performing a manipulation results in cross-site request forgery. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-1640	The Taskbuilder – WordPress Project Management & Task Management plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.0.2. This is due to missing authorization checks on the project and task comment submission functions (AJAX actions: wppm_submit_proj_comment and wppm_submit_task_comment). This makes it possible for authenticated attackers, with subscriber-level access and above, to create comments on any project or task (including private projects they cannot view or are not assigned to), and inject arbitrary HTML and CSS via the insufficiently sanitized comment_body parameter.	4.3	More Details
CVE-2025-12071	The Frontend User Notes plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.1.0 via the 'funp_ajax_modify_notes' AJAX endpoint due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify arbitrary notes that do not belong to them.	4.3	More Details
CVE-2026-20141	In Splunk Enterprise versions below 10.0.2, 10.0.3, 9.4.8, and 9.3.9, a low-privileged user who does not hold the "admin" Splunk role could access the Splunk Monitoring Console App endpoints due to an improper access control. This could lead to a sensitive information disclosure. The Monitoring Console app is a bundled app that comes with Splunk Enterprise. It is not available for download on SplunkBase, and is not installed on Splunk Cloud Platform instances. This vulnerability does not affect [Cloud Monitoring Console](https://help.splunk.com/en/splunk-cloud-platform/administer/admin-manual/10.2.2510/monitor-your-splunk-cloud-platform-deployment/introduction-to-the-cloud-monitoring-console).	4.3	More Details
CVE-2026-3043	A flaw has been found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/navbar.php. Executing a manipulation of the argument page can lead to cross site scripting. The attack may be performed from remote. The exploit has been published and may be used.	4.3	More Details
CVE-2026-2976	A weakness has been identified in FastApiAdmin up to 2.2.0. Affected by this issue is the function download_controller of the file /backend/app/api/v1/module_common/file/controller.py of the component Download Endpoint. This manipulation of the argument file_path causes information disclosure. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-27090	Cross-Site Request Forgery (CSRF) vulnerability in WP Moose Kenta Companion kenta-companion allows Cross Site Request Forgery.This issue affects Kenta Companion: from n/a through <= 1.3.3.	4.3	More Details
CVE-2026-26326	OpenClaw is a personal AI assistant. Prior to version 2026.2.14, `skills.status` could disclose secrets to `operator.read` clients by returning raw resolved config values in `configChecks` for skill `requires.config` paths. Version 2026.2.14 stops including raw resolved config values in requirement checks (return only `{ path, satisfied }`) and narrows the Discord skill requirement to the token key. In addition to upgrading, users should rotate any Discord tokens that may have been exposed to read-scoped clients.	4.3	More Details
CVE-2026-24241	NVIDIA Delegated Licensing Service for all appliance platforms contains a vulnerability where an attacker could exploit an improper authentication issue. A successful exploit of this vulnerability might lead to information disclosure.	4.3	More Details
CVE-2026-27511	Shenzhen Tenda F3 Wireless Router firmware V12.01.01.55_multi contains a clickjacking vulnerability in the web-based administrative interface. The interface does not set the X-Frame-Options header, allowing attacker-controlled sites to embed administrative pages in an iframe and trick an authenticated administrator into unintended interactions that may result in unauthorized configuration changes.	4.3	More Details
CVE-2026-27513	Shenzhen Tenda F3 Wireless Router firmware V12.01.01.55_multi contains a cross-site request forgery (CSRF) vulnerability in the web-based administrative interface. The interface does not implement anti-CSRF protections, allowing an attacker to induce an authenticated administrator to submit state-changing requests, which can result in unauthorized configuration changes.	4.3	More Details
CVE-2026-2386	The The Plus Addons for Elementor – Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Incorrect Authorization in all versions up to, and including, 6.4.7. This is due to the tpae_create_page() AJAX handler authorizing users only with current_user_can('edit_posts') while accepting a user-controlled 'post_type' value passed directly to wp_insert_post() without post-type-specific capability checks. This makes it possible for authenticated attackers, with Author-level access and above, to create arbitrary draft posts for restricted post types (e.g., 'page' and 'nxt_builder') via the 'post_type' parameter.	4.3	More Details
CVE-2026-	Missing Authorization vulnerability in uixthemes Sober sober allows Exploiting Incorrectly Configured Access Control Security	4.3	More

25459	Levels.This issue affects Sober: from n/a through <= 3.5.12.		Details
CVE-2026-27472	SPIP before 4.4.9 allows Blind Server-Side Request Forgery (SSRF) via syndicated sites in the private area. When editing a syndicated site, the application does not verify that the syndication URL is a valid remote URL, allowing an authenticated attacker to make the server issue requests to arbitrary internal or external destinations. This vulnerability is not mitigated by the SPIP security screen.	4.3	More Details
CVE-2026-23621	GFI MailEssentials AI versions prior to 22.4 contain an arbitrary directory existence enumeration vulnerability in the ListServer.IsPathExist() web method exposed at /MailEssentials/pages/MailSecurity/ListServer.aspx/IsPathExist. An authenticated user can supply an unrestricted filesystem path via the JSON key \"path\", which is URL-decoded and passed to Directory.Exists(), allowing the attacker to determine whether arbitrary directories exist on the server.	4.3	More Details
CVE-2026-23620	GFI MailEssentials AI versions prior to 22.4 contain an arbitrary file existence enumeration vulnerability in the ListServer.IsDBExist() web method exposed at /MailEssentials/pages/MailSecurity/ListServer.aspx/IsDBExist. An authenticated user can supply an unrestricted filesystem path via the JSON key \"path\", which is URL-decoded and passed to File.Exists(), allowing the attacker to determine whether arbitrary files exist on the server.	4.3	More Details
CVE-2025-71242	SPIP before 4.3.6, 4.2.17, and 4.1.20 allows unauthorized content disclosure in the private area. The application does not properly check authorization when displaying content of articles and sections (rubriques) in AJAX-loaded fragments, allowing an authenticated attacker to access restricted content. This vulnerability is not mitigated by the SPIP security screen.	4.3	More Details
CVE-2026-3027	A vulnerability was found in erzhongxmu JEEWMS up to 3.7. This affects an unknown part of the file src/main/webapp/plug-in/ueditor/jsp/getContent.jsp of the component UEditor. The manipulation of the argument myEditor results in cross site scripting. The attack can be launched 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.	4.3	More Details
CVE-2026-3028	A vulnerability was determined in erzhongxmu JEEWMS up to 3.7. This vulnerability affects the function doAdd of the file src/main/java/com/jeecg/demo/controller/JeecgListDemoController.java. This manipulation of the argument Name causes cross site scripting. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-2971	A vulnerability was found in a466350665 Smart-SSO up to 2.1.1. Affected by this issue is some unknown functionality of the file smart-sso-server/src/main/resources/templates/login.html of the component Login. Performing a manipulation of the argument redirectUri results in cross site scripting. The attack is possible to be carried out 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.	4.3	More Details
CVE-2026-26989	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below are affected by a Stored Cross-Site Scripting (XSS) vulnerability in the Alert Rules workflow. An attacker with administrative privileges can inject malicious scripts that execute in the browser context of any user who accesses the Alert Rules page. This issue has been fixed in version 26.2.0.	4.3	More Details
CVE-2026-27056	Missing Authorization vulnerability in StellarWP iThemes Sync ithemes-sync allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects iThemes Sync: from n/a through <= 3.2.8.	4.3	More Details
CVE-2026-2112	The Dam Spam plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.8. This is due to missing nonce verification on the pending comment deletion action in the cleanup page. This makes it possible for unauthenticated attackers to delete all pending comments via a forged request granted they can trick an admin into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-27055	Missing Authorization vulnerability in PenciDesign Penci AI SmartContent Creator penci-ai allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Penci AI SmartContent Creator: from n/a through <= 2.0.	4.3	More Details
CVE-2026-27100	Jenkins 2.550 and earlier, LTS 2.541.1 and earlier accepts Run Parameter values that refer to builds the user submitting the build does not have access to, allowing attackers with Item/Build and Item/Configure permission to obtain information about the existence of jobs, the existence of builds, and if a specified build exists, its display name.	4.3	More Details
CVE-2026-3049	A vulnerability was detected in horilla-opensource horilla up to 1.0.2. This issue affects the function get of the file horilla_generics/global_search.py of the component Query Parameter Handler. The manipulation of the argument prev_url results in open redirect. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 1.0.3 is capable of addressing this issue. The patch is identified as 730b5a44ff060916780c44a4bdbc8ced70a2cd27. The affected component should be upgraded.	4.3	More Details
CVE-2026-2943	A vulnerability was identified in SapneshNaik Student Management System up to f4b4f0928f0b5551a28ee81ae7e7fe47d9345318. This impacts an unknown function of the file index.php. Such manipulation of the argument Error leads to cross site scripting. The attack can be launched remotely. The exploit is publicly available and might be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-1860	The Kali Forms plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.4.8. This is due to the `get_items_permissions_check()` permission callback on the `/kaliforms/v1/forms/{id}` REST API endpoint only checking for the `edit_posts` capability without verifying that the requesting user has ownership or authorization over the specific form resource. This makes it possible for authenticated attackers, with Contributor-level access and above, to read form configuration data belonging to other users (including administrators) by enumerating form IDs. Exposed data includes form field structures, Google reCAPTCHA secret keys (if configured), email notification templates, and server paths.	4.3	More Details
CVE-2026-25318	Missing Authorization vulnerability in Wisernotify team WiserReview Product Reviews for WooCommerce wiser-review allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WiserReview Product Reviews for WooCommerce: from n/a through <= 2.9.	4.3	More Details

CVE-2026-27518	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior lack CSRF protections for state-changing actions in the administrative interface. An attacker can trick an authenticated administrator into performing unauthorized configuration changes.	4.3	More Details
CVE-2026-1369	The Conditional CAPTCHA WordPress plugin through 4.0.0 does not validate a parameter before redirecting the user to its value, leading to an Open Redirect issue	4.3	More Details
CVE-2026-1655	The EventPrime plugin for WordPress is vulnerable to unauthorized post modification due to missing authorization checks in all versions up to, and including, 4.2.8.4. This is due to the save_frontend_event_submission function accepting a user-controlled event_id parameter and updating the corresponding event post without enforcing ownership or capability checks. This makes it possible for authenticated (Customer+) attackers to modify posts created by administrators by manipulating the event_id parameter granted they can obtain a valid nonce.	4.3	More Details
CVE-2025-12075	The Order Splitter for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'wos_troubleshooting' AJAX endpoint in all versions up to, and including, 5.3.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view information pertaining to other user's orders.	4.3	More Details
CVE-2026-2633	The Gutenberg Blocks with AI by Kadence WP plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.6.1. This is due to a missing capability check in the `process_image_data_ajax_callback()` function which handles the `kadence_import_process_image_data` AJAX action. The function's authorization check via `verify_ajax_call()` only validates `edit_posts` capability but fails to check for the `upload_files` capability. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary images from remote URLs to the WordPress Media Library, bypassing the standard WordPress capability restriction that prevents Contributors from uploading files.	4.3	More Details
CVE-2026-2230	The Booking Calendar plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 10.14.14 via the handle_ajax_save function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, and booking permissions granted by an Administrator, to modify other users' plugin settings, such as booking calendar display options, which can disrupt the booking calendar functionality for the targeted user.	4.3	More Details
CVE-2026-20139	In Splunk Enterprise versions below 10.2.0, 10.0.2, 9.4.8, 9.3.9, and 9.2.12, and Splunk Cloud Platform versions below 10.2.2510.3, 10.1.2507.8, 10.0.2503.9, and 9.3.2411.121, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious payload into the `realname`, `tz`, or `email` parameters of the `/splunkd/__raw/services/authentication/users/username` REST API endpoint when they change a password. This could potentially lead to a client-side denial-of-service (DoS). The malicious payload might significantly slow page load times or render Splunk Web temporarily unresponsive.	4.3	More Details
CVE-2026-3054	A vulnerability was identified in Alinto SOGo 5.12.3/5.12.4. This impacts an unknown function. The manipulation of the argument hint leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-25419	Missing Authorization vulnerability in flycart UpsellWP checkout-upsell-and-order-bumps allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UpsellWP: from n/a through <= 2.2.3.	4.3	More Details
CVE-2026-25314	Missing Authorization vulnerability in WP Messiah TOP Table Of Contents top-table-of-contents allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TOP Table Of Contents: from n/a through <= 1.3.31.	4.3	More Details
CVE-2026-1072	The Keybase.io Verification plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.5. This is due to missing nonce validation when updating plugin settings. This makes it possible for unauthenticated attackers to update the Keybase verification text via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13438	The Page Title, Description & Open Graph Updater plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.02. This is due to missing nonce validation on multiple AJAX actions including dieno_update_page_title. This makes it possible for unauthenticated attackers to update page titles and metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14342	The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the sq_ajax_uninstall function in all versions up to, and including, 12.4.14. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the site from Squirrly's cloud service.	4.3	More Details
CVE-2026-25003	Missing Authorization vulnerability in madalin.ungureanu Client Portal client-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Portal: from n/a through <= 1.2.1.	4.3	More Details
CVE-2019-25451	phpMoAdmin 1.1.5 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized database operations by crafting malicious requests. Attackers can trick authenticated users into submitting GET requests to moadmin.php with parameters like action, db, and collection to create, drop, or repair databases and collections without user consent.	4.3	More Details
CVE-2025-13413	The Country Blocker for AdSense plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the CBFA_guardar_cbfa() function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2019-25447	OrientDB 3.0.17 GA Community Edition contains cross-site request forgery vulnerabilities that allow attackers to perform unauthorized actions by crafting malicious requests to endpoints like /database/, /command/, and /document/. Attackers can create or delete databases, modify schema classes, manage users, and create functions by sending authenticated requests without token validation, combined with reflected and stored cross-site scripting vulnerabilities in the web interface.	4.3	More Details

CVE-2026-1925	The EmailKit – Email Customizer for WooCommerce & WP plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the 'update_template_data' function in all versions up to, and including, 1.6.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the title of any post on the site, including posts, pages, and custom post types.	4.3	More Details
CVE-2026-2683	A vulnerability was found in Tsinghua Unigroup Electronic Archives System 3.2.210802(62532). The affected element is an unknown function of the file /Using/Subject/downLoad.html. Performing a manipulation of the argument path results in path traversal. The attack may be initiated 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.	4.3	More Details
CVE-2025-14427	The Shield Security: Blocks Bots, Protects Users, and Prevents Security Breaches plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `MfaEmailDisable` action in all versions up to, and including, 21.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disable the global Email 2FA setting for the entire site.	4.3	More Details
CVE-2025-12027	The Mesmerize Companion plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the "openPageInCustomizer" and "openPageInDefaultEditor" functions in all versions up to, and including, 1.6.158. This makes it possible for authenticated attackers - with subscriber level access and above, on websites with the Mesmerize theme activated - to mark arbitrary pages as maintainable, wrap their content in custom sections, change page template metadata, and toggle the default editor flag without proper authorization.	4.3	More Details
CVE-2026-24314	Under certain conditions SAP S/4HANA (Manage Payment Media) allows an authenticated attacker to access information which would otherwise be restricted. This could cause low impact on confidentiality of the application while integrity and availability are not impacted.	4.3	More Details
CVE-2025-12356	The Tickera – Sell Tickets & Manage Events plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_change_ticket_status' AJAX endpoint in all versions up to, and including, 3.5.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update post/event statuses.	4.3	More Details
CVE-2025-14864	The Virusdie - One-click website security plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.7. This is due to missing capability checks on the `vd_get_apikey` function which is hooked to `wp_ajax_virusdie_apikey`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve the site's Virusdie API key, which could be used to access the site owner's Virusdie account and potentially compromise site security.	4.3	More Details
CVE-2025-12081	The ACF Photo Gallery Field plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the "acf_photo_gallery_edit_save" function in all versions up to, and including, 3.0. This makes it possible for authenticated attackers, with subscriber level access and above, to modify the title, caption, and custom metadata of arbitrary media attachments.	4.3	More Details
CVE-2026-2705	A vulnerability was detected in Open Babel up to 3.1.1. The impacted element is the function OBAtom::SetFormalCharge in the library include/openbabel/atom.h of the component MOL2 File Handler. The manipulation results in out-of-bounds read. It is possible to launch the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-2704	A security vulnerability has been detected in Open Babel up to 3.1.1. The affected element is the function OpenBabel::transform3d::DescribeAsString of the file src/math/transform3d.cpp of the component CIF File Handler. The manipulation leads to out-of-bounds read. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2025-12172	The Mailchimp List Subscribe Form plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.0. This is due to missing or incorrect nonce validation on the mailchimp_sf_change_list_if_necessary() function. This makes it possible for unauthenticated attackers to change Mailchimp lists via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13091	The Shopire theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the shopire_admin_install_plugin() function in all versions up to, and including, 1.0.57. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the 'fable-extra' plugin.	4.3	More Details
CVE-2026-27741	Bludit version 3.16.1 contains a cross-site request forgery (CSRF) vulnerability in the /admin/uninstall-plugin/ and /admin/install-theme/ endpoints. The application does not implement anti-CSRF tokens or other request origin validation mechanisms for these administrative actions. An attacker can induce an authenticated administrator to visit a malicious page that silently submits crafted requests, resulting in unauthorized plugin uninstallation or theme installation. This may lead to loss of functionality, execution of untrusted code via malicious themes, and compromise of system integrity.	4.3	More Details
CVE-2026-2693	A vulnerability was determined in CoCoTeaNet CyreneAdmin up to 1.3.0. This vulnerability affects unknown code of the file /api/system/dashboard/getCount of the component System Info Endpoint. Executing a manipulation can lead to improper authorization. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-1455	The Whatsiplus Scheduled Notification for Woocommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing nonce validation on the 'wsnfw_save_users_settings' AJAX action. This makes it possible for unauthenticated attackers to modify plugin configuration settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-2692	A vulnerability was found in CoCoTeaNet CyreneAdmin up to 1.3.0. This affects an unknown part of the file /api/system/user/getAvatar of the component Image Handler. Performing a manipulation of the argument Avatar results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-12884	The Advanced Ads – Ad Manager & AdSense plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 2.0.14. This is due to the plugin not properly verifying that a user is authorized to perform an action in the `placement_update_item()` function. This makes it possible for authenticated attackers, with subscriber-level access and above, to update ad placements, allowing them to change which ad or ad group a placement serves.	4.3	More Details

CVE-2026-25008	Insertion of Sensitive Information Into Sent Data vulnerability in Shahjahan Jewel Ninja Tables ninja-tables allows Retrieve Embedded Sensitive Data.This issue affects Ninja Tables: from n/a through <= 5.2.5.	4.3	More Details
CVE-2026-2504	The Dealia – Request a quote plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on multiple AJAX handlers in all versions up to, and including, 1.0.6. The admin nonce (DEALIA_ADMIN_NONCE) is exposed to all users with edit_posts capability (Contributor+) via wp_localize_script() in PostsController.php, while the AJAX handlers in AdminSettingsController.php only verify the nonce without checking current_user_can('manage_options'). This makes it possible for authenticated attackers, with Contributor-level access and above, to reset the plugin configuration.	4.3	More Details
CVE-2026-25308	Missing Authorization vulnerability in wp.insider Simple Membership simple-membership allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simple Membership: from n/a through <= 4.6.9.	4.3	More Details
CVE-2025-14167	The Remove Post Type Slug plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to incorrect nonce validation logic that uses OR (||) instead of AND (&&), causing the validation to fail when the nonce field is not empty OR when verification fails, rather than when it's empty AND verification fails. This makes it possible for unauthenticated attackers to modify the plugin's post type slug removal settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-25313	Missing Authorization vulnerability in Shahjahan Jewel FluentForm fluentform allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FluentForm: from n/a through <= 6.1.14.	4.3	More Details
CVE-2026-1906	The PDF Invoices & Packing Slips for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.6.0 via the `wpo_ips_edi_save_order_customer_peppol_identifiers` AJAX action due to missing capability checks and order ownership validation. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify Peppol/EDI endpoint identifiers (`peppol_endpoint_id`, `peppol_endpoint_eas`) for any customer by specifying an arbitrary `order_id` parameter on systems using Peppol invoicing. This can affect order routing on the Peppol network and may result in payment disruptions and data leakage.	4.3	More Details
CVE-2026-3070	A vulnerability was detected in SourceCodester Modern Image Gallery App 1.0. Affected by this vulnerability is an unknown functionality of the file upload.php. The manipulation of the argument filename results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-2802	Race condition in the JavaScript: GC component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	4.2	More Details
CVE-2025-61146	saitoha libsixel until v1.8.7 was discovered to contain a memory leak via the component malloc_stub.c.	4.0	More Details
CVE-2026-27576	OpenClaw is a personal AI assistant. In versions 2026.2.17 and below, the ACP bridge accepts very large prompt text blocks and can assemble oversized prompt payloads before forwarding them to chat.send. Because ACP runs over local stdio, this mainly affects local ACP clients (for example IDE integrations) that send unusually large inputs. This issue has been fixed in version 2026.2.19.	4.0	More Details
CVE-2026-26365	Akamai Ghost on Akamai CDN edge servers before 2026-02-06 mishandles processing of custom hop-by-hop HTTP headers, where an incoming request containing the header "Connection: Transfer-Encoding" could result in a forward request with invalid message framing, depending on the Akamai processing path. This could result in the origin server parsing the request body incorrectly, leading to HTTP request smuggling.	4.0	More Details
CVE-2025-15589	A vulnerability was determined in MuYuCMS 2.7. Affected is the function delete_dir_file of the file application/admin/controller/Template.php of the component Template Management Page. This manipulation of the argument temn/tp causes path traversal. 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.	3.8	More Details
CVE-2026-2733	A flaw was identified in the Docker v2 authentication endpoint of Keycloak, where tokens continue to be issued even after a Docker registry client has been administratively disabled. This means that turning the client “Enabled” setting to OFF does not fully prevent access. As a result, previously valid credentials can still be used to obtain authentication tokens. This weakens administrative controls and could allow unintended access to container registry resources.	3.8	More Details
CVE-2026-25423	Missing Authorization vulnerability in creativeinteractivemedia Real 3D FlipBook real3d-flipbook-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Real 3D FlipBook: from n/a through <= 4.16.4.	3.8	More Details
CVE-2026-2967	A security vulnerability has been detected in Cesanta Mongoose up to 7.20. This affects the function getpeer of the file /src/net_builtin.c of the component TCP Sequence Number Handler. The manipulation leads to improper verification of source of a communication channel. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is reported as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2026-22885	A vulnerability exists in EnOcean SmartServer IoT version 4.60.009 and prior, which would allow remote attackers, in the LON IP-852 management messages, to send specially crafted IP-852 messages resulting in a memory leak from the program's memory.	3.7	More Details
CVE-2026-2895	A security flaw has been discovered in funadmin up to 7.1.0-rc4. Affected by this issue is the function repass of the file app/frontend/controller/Member.php. Performing a manipulation of the argument forget_code/vercode results in weak password recovery. Remote exploitation of the attack is possible. The attack's complexity is rated as high. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details

CVE-2026-24122	Cosign provides code signing and transparency for containers and binaries. In versions 3.0.4 and below, an issuing certificate with a validity that expires before the leaf certificate will be considered valid during verification even if the provided timestamp would mean the issuing certificate should be considered expired. When verifying artifact signatures using a certificate, Cosign first verifies the certificate chain using the leaf certificate's "not before" timestamp and later checks expiry of the leaf certificate using either a signed timestamp provided by the Rekor transparency log or from a timestamp authority, or using the current time. The root and all issuing certificates are assumed to be valid during the leaf certificate's validity. There is no impact to users of the public Sigstore infrastructure. This may affect private deployments with customized PKIs. This issue has been fixed in version 3.0.5.	3.7	More Details
CVE-2026-1582	The WP All Export plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.14 via the export download endpoint. This is due to a PHP type juggling vulnerability in the security token comparison which uses loose comparison (==) instead of strict comparison (===). This makes it possible for unauthenticated attackers to bypass authentication using "magic hash" values when the expected MD5 hash prefix happens to be numeric-looking (matching pattern ^0e\d+$), allowing download of sensitive export files containing PII, business data, or database information.	3.7	More Details
CVE-2026-24764	OpenClaw (formerly Clawdbot) is a personal AI assistant users run on their own devices. In versions 2026.2.2 and below, when the Slack integration is enabled, channel metadata (topic/description) can be incorporated into the model's system prompt. Prompt injection is a documented risk for LLM-driven systems. This issue increases the injection surface by allowing untrusted Slack channel metadata to be treated as higher-trust system input. This issue has been fixed in version 2026.2.3.	3.7	More Details
CVE-2026-2966	A weakness has been identified in Cesanta Mongoose up to 7.20. The impacted element is the function mg_sendnsreq of the file /src/dns.c of the component DNS Transaction ID Handler. Executing a manipulation of the argument random can lead to insufficiently random values. The attack can be launched remotely. The attack requires a high level of complexity. The exploitability is regarded as difficult. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2026-2968	A vulnerability was detected in Cesanta Mongoose up to 7.20. This impacts the function mg_chacha20_poly1305_decrypt of the file /src/tls_chacha20.c of the component Poly1305 Authentication Tag Handler. The manipulation results in improper verification of cryptographic signature. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is said to be difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2026-2709	A flaw has been found in busy up to 2.5.5. The affected element is an unknown function of the file source-code/busy-master/src/server/app.js of the component Callback Handler. Executing a manipulation of the argument state can lead to open redirect. It is possible to launch the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-2825	A vulnerability has been found in rachelos WeRSS we-mp-rss up to 1.4.8. This impacts the function fix_html of the file tools/fix.py of the component Article Module. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-3050	A flaw has been found in horilla-opensource horilla up to 1.0.2. Impacted is an unknown function of the file static/assets/js/global.js of the component Leads Module. This manipulation of the argument Notes causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. Upgrading to version 1.0.3 is recommended to address this issue. Patch name: fc5c8e55988e89273012491b5f097b762b474546. It is suggested to upgrade the affected component.	3.5	More Details
CVE-2026-20137	In Splunk Enterprise versions below 10.2.0, 10.0.3, 9.4.5, 9.3.7, and 9.2.9, and Splunk Cloud Platform versions below 10.1.2507.0, 10.0.2503.9, 9.3.2411.112, and 9.3.2408.122, a low-privileged user who does not hold the "admin" or "power" Splunk roles could bypass the SPL safeguards for risky commands when they create a Data Model that contains an injected SPL query within an object. They can bypass the safeguards by exploiting a path traversal vulnerability.	3.5	More Details
CVE-2026-2947	A vulnerability was detected in rymcu forest up to 0.0.5. This affects the function updateUserInfo of the file - src/main/java/com/rymcu/forest/web/api/user/UserInfoController.java of the component User Profile Handler. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-52603	HCL Connections is vulnerable to information disclosure. In a very specific user navigation scenario, this could allow a user to obtain limited information when a single piece of internal metadata is returned in the browser.	3.5	More Details
CVE-2025-15583	A weakness has been identified in detronetdip E-commerce 1.0.0. This affects the function get_safe_value of the file utility/function.php. 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 project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-2946	A security vulnerability has been detected in rymcu forest up to 0.0.5. Affected by this issue is the function XssUtils.replaceHtmlCode of the file src/main/java/com/rymcu/forest/util/XssUtils.java of the component Article Content/Comments/Portfolio. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-2703	A weakness has been identified in xlnt-community xlnt up to 1.6.1. Impacted is the function xlnt::detail::decode_base64 of the file source/detail/cryptography/base64.cpp of the component Encrypted XLSX File Parser. Executing a manipulation can lead to off-by-one. The attack requires local access. The exploit has been made available to the public and could be used for attacks. This patch is called f2d7bf494e5c52706843cf7eb9892821bffb0734. Applying a patch is advised to resolve this issue.	3.3	More Details
CVE-2026-2659	A vulnerability was determined in Squirrel up to 3.2. Affected by this vulnerability is the function SQFuncState::PopTarget of the file src/squirrel/squirrel/sqfuncstate.cpp. Executing a manipulation of the argument _target_stack can lead to out-of-bounds read. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details

CVE-2026-27007	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, `normalizeForHash` in `src/agents/sandbox/config-hash.ts` recursively sorted arrays that contained only primitive values. This made order-sensitive sandbox configuration arrays hash to the same value even when order changed. In OpenClaw sandbox flows, this hash is used to decide whether existing sandbox containers should be recreated. As a result, order-only config changes (for example Docker `dns` and `binds` array order) could be treated as unchanged and stale containers could be reused. This is a configuration integrity issue affecting sandbox recreation behavior. Starting in version 2026.2.15, array ordering is preserved during hash normalization; only object key ordering remains normalized for deterministic hashing.	3.3	More Details
CVE-2026-2887	A security vulnerability has been detected in aardappel lobster up to 2025.4. This impacts the function lobster::TypeName in the library dev/src/lobster/idents.h. Such manipulation leads to uncontrolled recursion. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used. Upgrading to version 2026.1 will fix this issue. The name of the patch is 8ba49f98ccfc9734ef352146806433a41d9f9aa6. It is advisable to upgrade the affected component.	3.3	More Details
CVE-2026-2889	A vulnerability was detected in CCExtractor up to 0.96.5. Affected is the function processmp4 in the library src/lib_ccx/mp4.c. Performing a manipulation results in use after free. The attack is only possible with local access. The exploit is now public and may be used. Upgrading to version 0.96.6 is able to address this issue. The patch is named fd7271bae238ccb3ae8a71304ea64f0886324925. You should upgrade the affected component.	3.3	More Details
CVE-2026-2644	A weakness has been identified in niklasso minisat up to 2.2.0. This issue affects the function Solver::value in the library core/SolverTypes.h of the component DIMACS File Parser. This manipulation of the argument variable index with the input 2147483648 causes out-of-bounds read. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2903	A flaw has been found in skvadrik re2c up to 4.4. Impacted is the function check_and_merge_special_rules of the file src/parse/ast.cc. This manipulation causes null pointer dereference. The attack can only be executed locally. The exploit has been published and may be used. Patch name: febeb977936f9519a25d9fbd10ff8256358cdb97. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2026-2657	A vulnerability has been found in wren-lang wren up to 0.4.0. This impacts the function printError of the file src/vm/wren_compiler.c of the component Error Message Handler. Such manipulation leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2661	A security flaw has been discovered in Squirrel up to 3.2. This affects the function SQObjectPtr::operator in the library squirrel/sqobject.h. The manipulation results in heap-based buffer overflow. The attack needs to be approached locally. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2642	A security vulnerability has been detected in ggreer the_silver_searcher up to 2.2.0. The impacted element is the function search_stream of the file src/search.c. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2660	A vulnerability was identified in FascinatedBox lily up to 2.3. Affected by this issue is the function shorthash_for_name of the file src/lily_symtab.c. The manipulation leads to use after free. Local access is required to approach this attack. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2662	A weakness has been identified in FascinatedBox lily up to 2.3. This vulnerability affects the function count_transforms of the file src/lily_emitter.c. This manipulation causes out-of-bounds read. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2025-8860	A flaw was found in QEMU in the uefi-vars virtual device. When the guest writes to register UEFI_VARS_REG_BUFFER_SIZE, the .write callback `uefi_vars_write` is invoked. The function allocates a heap buffer without zeroing the memory, leaving the buffer filled with residual data from prior allocations. When the guest later reads from register UEFI_VARS_REG_PIO_BUFFER_TRANSFER, the .read callback `uefi_vars_read` returns leftover metadata or other sensitive process memory from the previously allocated buffer, leading to an information disclosure vulnerability.	3.3	More Details
CVE-2026-2641	A weakness has been identified in universal-ctags ctags up to 6.2.1. The affected element is the function parseExpression/parseExprList of the file parsers/v.c of the component V Language Parser. Executing a manipulation can lead to uncontrolled recursion. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2869	A vulnerability was identified in janet-lang janet up to 1.40.1. Affected by this vulnerability is the function janetc_varset of the file src/core/specials.c of the component handleattr Handler. The manipulation leads to out-of-bounds read. The attack can only be performed from a local environment. The exploit is publicly available and might be used. Upgrading to version 1.41.0 addresses this issue. The identifier of the patch is 2fabc80151a2b8834ee59cda8a70453f848b40e5. The affected component should be upgraded.	3.3	More Details
CVE-2025-12343	A flaw was found in FFmpeg's TensorFlow backend within the libavfilter/dnn_backend_tf.c source file. The issue occurs in the dnn_execute_model_tf() function, where a task object is freed multiple times in certain error-handling paths. This redundant memory deallocation can lead to a double-free condition, potentially causing FFmpeg or any application using it to crash when processing TensorFlow-based DNN models. This results in a denial-of-service scenario but does not allow arbitrary code execution under normal conditions.	3.3	More Details
CVE-2026-2858	A vulnerability was identified in wren-lang wren up to 0.4.0. This affects the function peekChar of the file src/vm/wren_compiler.c of the component Source File Parser. Such manipulation leads to out-of-bounds read. The attack needs to be performed locally. The exploit is publicly available and might be used. The project was informed of the problem early	3.3	More Details

	through an issue report but has not responded yet.		
CVE-2026-2702	A security flaw has been discovered in Beetel 777VR1 up to 01.00.09. This issue affects some unknown processing of the component WPA2 PSK. Performing a manipulation results in hard-coded credentials. The attacker must have access to the local network to execute the attack. The complexity of an attack is rather high. The exploitability is assessed as difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-27171	zlib before 1.3.2 allows CPU consumption via crc32_combine64 and crc32_combine_gen64 because x2nmodp can do right shifts within a loop that has no termination condition.	2.9	More Details
CVE-2026-1831	The YayMail - WooCommerce Email Customizer plugin for WordPress is vulnerable to unauthorized plugin installation and activation due to missing capability checks on the 'yaymail_install_yaysmtp' AJAX action and `/yaymail/v1/addons/activate` REST endpoint in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to install and activate the YaySMTP plugin.	2.7	More Details
CVE-2026-2419	The WP-DownloadManager plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.69 via the 'download_path' configuration parameter. This is due to insufficient validation of the download path setting, which allows directory traversal sequences to bypass the WP_CONTENT_DIR prefix check. This makes it possible for authenticated attackers, with Administrator-level access and above, to configure the plugin to list and access arbitrary files on the server by exploiting the file browser functionality.	2.7	More Details
CVE-2026-23859	Dell Wyse Management Suite, versions prior to WMS 5.5, contain a Client-Side Enforcement of Server-Side Security vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability to Protection mechanism bypass.	2.7	More Details
CVE-2026-26964	Windmill is an open-source developer platform for internal code: APIs, background jobs, workflows and UIs. Versions 1.634.6 and below allow non-admin users to obtain Slack OAuth client secrets, which should only be accessible to workspace administrators. The GET /api/w/{workspace}/workspaces/get_settings endpoint returns the slack_oauth_client_secret to any authenticated workspace member, regardless of their admin status. It is expected behavior for non-admin users see a redacted version of workspace settings, as some of them are necessary for the frontend to behave correctly even for non-admins. However, the Slack configuration should not be visible to non-admins. This is a legacy issue where the setting was stored as a plain value instead of using $variable indirection, and it was never added to the redaction logic. This issue has been fixed in version 1.635.0.	2.7	More Details
CVE-2025-14270	The OneClick Chat to Order plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 1.0.9. This is due to the plugin not properly verifying that a user is authorized to perform an action in the wa_order_number_save_number_field function. This makes it possible for authenticated attackers, with Editor-level access and above, to modify WhatsApp phone numbers used by the plugin, redirecting customer orders and messages to attacker-controlled phone numbers.	2.7	More Details
CVE-2026-25120	Gogs is an open source self-hosted Git service. In versions 0.13.4 and below, the DeleteComment API does not verify that the comment belongs to the repository specified in the URL. This allows a repository administrator to delete comments from any other repository by supplying arbitrary comment IDs, bypassing authorization controls. The DeleteComment function retrieves a comment by ID without verifying repository ownership and the Database function DeleteCommentByID performs no repository validation. This issue has been fixed in version 0.14.0.	2.7	More Details
CVE-2026-2656	A flaw has been found in ChaiScript up to 6.1.0. This affects the function chaiscript::Type_Info::bare_equal of the file include/chaiscript/dispatchkit/type_info.hpp. This manipulation causes use after free. The attack requires local access. The attack's complexity is rated as high. The exploitability is reported as difficult. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2.5	More Details
CVE-2026-2655	A vulnerability was detected in ChaiScript up to 6.1.0. The impacted element is the function chaiscript::str_less::operator of the file include/chaiscript/chaiscript_defines.hpp. The manipulation results in use after free. The attack requires a local approach. The attack requires a high level of complexity. The exploitability is regarded as difficult. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2.5	More Details
CVE-2026-2913	A vulnerability was determined in libvips up to 8.19.0. The affected element is the function vips_source_read_to_memory of the file libvips/iofuncs/source.c. This manipulation causes heap-based buffer overflow. It is possible to launch the attack on the local host. The attack's complexity is rated as high. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. Patch name: a56feecbe9ed66521d9647ec9fbcd2546eccd7ee. Applying a patch is the recommended action to fix this issue. The confirmation of the bugfix mentions: "[T]he impact of this is negligible, since this only affects custom seekable sources larger than 4 GiB (and the crash occurs in user code rather than libvips itself)."	2.5	More Details
CVE-2026-2974	A vulnerability was identified in AliasVault App up to 0.25.3 on Android/iOS. This vulnerability affects unknown code of the file shared_prefs/aliasvault.xml of the component Backup Handler. The manipulation of the argument accessToken/refreshToken/metadata/key_derivation_params/auth_methods leads to exposure of backup file to an unauthorized control sphere. An attack has to be approached locally. The attack is considered to have high complexity. It is stated that the exploitability is difficult. The exploit is publicly available and might be used. Upgrading to version 0.26.0 is able to resolve this issue. The identifier of the patch is 873ecc03f92238e162f98a068ad56069a922b4f6/0bd662320174d8265dfe3b05a04bc13efc960532. It is recommended to upgrade the affected component. The creator of the software explains: "Because of AliasVault's zero-knowledge encryption design, the tokens stored in aliasvault.xml are API session tokens that cannot decrypt the vault on their own: the master password is required for that. So while this isn't a direct vault compromise risk, there's no reason to include them in backups either."	2.5	More Details
CVE-2026-2933	A weakness has been identified in YiFang CMS up to 2.0.5. This affects the function update of the file app/db/admin/D_adManage.php of the component Extended Management Module. Executing a manipulation of the argument Name can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2.4	More Details

CVE-2026-2897	A security vulnerability has been detected in funadmin up to 7.1.0-rc4. This vulnerability affects unknown code of the file app/backend/view/index/index.html of the component Backend Interface. The manipulation of the argument Value leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-2939	A vulnerability was found in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /add_student/ of the component Add Student Module. 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.	2.4	More Details
CVE-2026-2932	A security flaw has been discovered in YiFang CMS up to 2.0.5. The impacted element is the function update of the file app/db/admin/D_adPosition.php of the component Extended Management Module. Performing a manipulation of the argument name/index results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	2.4	More Details
CVE-2026-2972	A vulnerability was determined in a466350665 Smart-SSO up to 2.1.1. This affects the function Save of the file smart-sso-server/src/main/java/openjoe/smart/sso/server/controller/admin/UserController.java of the component Role Edit Page. Executing a manipulation can lead to cross site scripting. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-3041	A security vulnerability has been detected in xingfuggz BaykeShop up to 1.3.20. Impacted is an unknown function of the file src/baykeshop/contrib/article/templates/baykeshop/sidebar/custom.html of the component Article Sidebar Module. Such manipulation of the argument sidebar.content leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2.4	More Details
CVE-2026-2934	A security vulnerability has been detected in YiFang CMS up to 2.0.5. This impacts the function update of the file app/db/admin/D_friendLinkGroup.php of the component Extended Management Module. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2026-2965	A security flaw has been discovered in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 1.2.9. The affected element is an unknown function of the file /admin/SysModule/edit.html of the component System Extension Module. Performing a manipulation of the argument Title results in cross site scripting. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-27467	BigBlueButton is an open-source virtual classroom. In versions 3.0.19 and below, when first joining a session with the microphone muted, the client sends audio to the server regardless of mute state. Media is discarded at the server side, so it isn't audible to any participants, but this may allow for malicious server operators to access audio data. The behavior is only incorrect between joining the meeting and the first time the user unmutes. This issue has been fixed in version 3.0.20.	2.0	More Details
CVE-2025-1787	Local admin could to leak information from the Genetec Update Service configuration web page. An authenticated, admin privileged, Windows user could exploit this vulnerability to gain elevated privileges in the Genetec Update Service. Could be combined with CVE-2025-1789 to achieve low privilege escalation.	N/A	More Details
CVE-2026-1768	A permission cache poisoning vulnerability in Devolutions Server allows authenticated users to bypass permissions to access entries.This issue affects Devolutions Server: before 2025.3.15.	N/A	More Details
CVE-2026-21665	The Print Service component of Fiserv Originate Loans Peripherals (formerly Velocity Services) in unsupported version 2021.2.4 (build 4.7.3155.0011) uses deprecated .NET Remoting TCP channels that allow unsafe deserialization of untrusted data. When these services are exposed to an untrusted network in a client-managed deployment, an unauthenticated attacker can achieve remote code execution. Version 2021.2.4 is no longer supported by Fiserv. Customers should upgrade to a currently supported release (2025.1 or later) and ensure that .NET Remoting service ports are not exposed beyond trusted network boundaries. This CVE documents behavior observed in a client-hosted deployment running an unsupported legacy version of Originate Loans Peripherals with .NET Remoting ports exposed to an untrusted network. This is not a default or supported configuration. Customers running legacy versions should upgrade to a currently supported release and ensure .NET Remoting ports are restricted to trusted network segments. The finding does not apply to Fiserv-hosted environments.	N/A	More Details
CVE-2026-25501	free5GC SMF provides Session Management Function for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, SMF panics due to nil pointer dereference and the SMF process terminates. This is triggered by a malformed PFCP SessionReportRequest on the SMF PFCP (UDP/8805) interface. No known upstream fix is available, but some workarounds are available. ACL/firewall the PFCP interface so only trusted UPF IPs can reach SMF (reduce spoofing/abuse surface); drop/inspect malformed PFCP SessionReportRequest messages at the network edge where feasible, and/or add recover() around PFCP handler dispatch to avoid whole-process termination (mitigation only).	N/A	More Details
CVE-2025-1789	Local privilege escalation in Genetec Update Service. An authenticated, low-privileged, Windows user could exploit this vulnerability to gain elevated privileges on the affected system.	N/A	More Details
CVE-2026-27572	Wasmtime is a runtime for WebAssembly. Prior to versions 24.0.6, 36.0.6, 4.0.04, 41.0.4, and 42.0.0, Wasmtime's implementation of the `wasi:http/types.fields` resource is susceptible to panics when too many fields are added to the set of headers. Wasmtime's implementation in the `wasmtime-wasi-http` crate is backed by a data structure which panics when it reaches excessive capacity and this condition was not handled gracefully in Wasmtime. Panicking in a WASI implementation is a Denial of Service vector for embedders and is treated as a security vulnerability in Wasmtime. Wasmtime 24.0.6, 36.0.6, 40.0.4, 41.0.4, and 42.0.0 patch this vulnerability and return a trap to the guest instead of panicking. There are no known workarounds at this time. Embedders are encouraged to update to a patched version of Wasmtime.	N/A	More Details
CVE-2026-2757	Incorrect boundary conditions in the WebRTC: Audio/Video component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details

CVE-2026-27035	Rejected reason: Not used	N/A	More Details
CVE-2026-27036	Rejected reason: Not used	N/A	More Details
CVE-2026-27037	Rejected reason: Not used	N/A	More Details
CVE-2026-25545	Astro is a web framework. Prior to version 9.5.4, Server-Side Rendered pages that return an error with a prerendered custom error page (eg. `404.astro` or `500.astro`) are vulnerable to SSRF. If the `Host:` header is changed to an attacker's server, it will be fetched on `/500.html` and they can redirect this to any internal URL to read the response body through the first request. An attacker who can access the application without `Host:` header validation (eg. through finding the origin IP behind a proxy, or just by default) can fetch their own server to redirect to any internal IP. With this they can fetch cloud metadata IPs and interact with services in the internal network or localhost. For this to be vulnerable, a common feature needs to be used, with direct access to the server (no proxies). Version 9.5.4 fixes the issue.	N/A	More Details
CVE-2026-1772	RTU500 web interface: An unprivileged user can read user management information. The information cannot be accessed via the RTU500 web user interface but requires further tools like browser development utilities to access them without required privileges.	N/A	More Details
CVE-2026-25882	Fiber is an Express inspired web framework written in Go. A denial of service vulnerability exists in Fiber v2 and v3 that allows remote attackers to crash the application by sending requests to routes with more than 30 parameters. The vulnerability results from missing validation during route registration combined with an unbounded array write during request matching. Version 2.52.12 patches the issue in the v2 branch and 3.1.0 patches the issue in the v3 branch.	N/A	More Details
CVE-2026-3061	Out of bounds read in Media in Google Chrome prior to 145.0.7632.116 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2026-26340	Tattile Smart+, Vega, and Basic device families firmware versions 1.181.5 and prior expose RTSP streams without requiring authentication. A remote attacker can connect to the RTSP service and access live video/audio streams without valid credentials, resulting in unauthorized disclosure of surveillance data.	N/A	More Details
CVE-2026-23980	Improper Neutralization of Special Elements used in a SQL Command ('SQL Injection') vulnerability in Apache Superset allows an authenticated user with read access to conduct error-based SQL injection via the sqlExpression or where parameters. This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue.	N/A	More Details
CVE-2026-23983	A Sensitive Data Exposure vulnerability exists in Apache Superset allowing authenticated users to retrieve sensitive user information. The Tag endpoint (disabled by default) allows users to retrieve a list of objects associated with a specific tag. When these associated objects include Users, the API response improperly serializes and returns sensitive fields, including password hashes (pbkdf2), email addresses, and login statistics. This vulnerability allows authenticated users with low privileges (e.g., Gamma role) to view sensitive authentication data This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue or make sure TAGGING_SYSTEM is False (Apache Superset current default)	N/A	More Details
CVE-2026-23969	Apache Superset utilizes a configurable dictionary, DISALLOWED_SQL_FUNCTIONS, to restrict the execution of potentially sensitive SQL functions within SQL Lab and charts. While this feature included restrictions for engines like PostgreSQL, a vulnerability was reported where the default list for the ClickHouse engine was incomplete. This issue affects Apache Superset: before 4.1.2. Users are recommended to upgrade to version 4.1.2, which fixes the issue.	N/A	More Details
CVE-2026-2759	Incorrect boundary conditions in the Graphics: ImageLib component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-24443	EventSentry versions prior to 6.0.1.20 contain an unverified password change vulnerability in the account management functionality of the Web Reports interface. The password change mechanism does not require validation of the current password before allowing a new password to be set. An attacker who gains temporary access to an authenticated user session can change the account password without knowledge of the original credentials. This enables persistent account takeover and, if administrative accounts are affected, may result in privilege escalation.	N/A	More Details
CVE-2026-3131	Improper access control in multiple DVLS REST API endpoints in Devolutions Server 2025.3.14.0 and earlier allows an authenticated user with view-only permission to access sensitive connection data.	N/A	More Details
CVE-2026-27032	Rejected reason: Not used	N/A	More Details
CVE-2026-23984	An Improper Input Validation vulnerability exists in Apache Superset that allows an authenticated user with SQLLab access to bypass the read-only verification check when using a PostgreSQL database connection. While the system effectively blocks standard Data Manipulation Language (DML) statements (e.g., INSERT, UPDATE, DELETE) on read-only connections, it fails to detect them in specially crafted SQL statements. This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue.	N/A	More Details
CVE-2026-	Mastodon is a free, open-source social network server based on ActivityPub. FASP registration requires manual approval by an administrator. In versions 4.4.0 through 4.4.13 and 4.5.0 through 4.5.6, an unauthenticated attacker can register a FASP with an attacker-chosen `base_url` that includes or resolves to a local / internal address, leading to the Mastodon server making requests to that address. This only affects Mastodon servers that have opted in to testing the experimental FASP feature by setting the environment variable `EXPERIMENTAL_FEATURES` to a value including `fasp`. An attacker can force the Mastodon	N/A	More

27477	server to make http(s) requests to internal systems. While they cannot control the full URL that is being requested (only the prefix) and cannot see the result of those requests, vulnerabilities or other undesired behavior could be triggered in those systems. The fix is included in the 4.4.14 and 4.5.7 releases. Admins that are actively testing the experimental "fasp" feature should update their systems. Servers not using the experimental feature flag `fasp` are not affected.		Details
CVE-2026-25891	Fiber is an Express inspired web framework written in Go. A Path Traversal (CWE-22) vulnerability in Fiber allows a remote attacker to bypass the static middleware sanitizer and read arbitrary files on the server file system on Windows. This affects Fiber v3 through version 3.0.0. This has been patched in Fiber v3 version 3.1.0.	N/A	More Details
CVE-2026-27031	Rejected reason: Not used	N/A	More Details
CVE-2026-26342	Tattile Smart+, Vega, and Basic device families firmware versions 1.181.5 and prior implement an authentication token (X-User-Token) with insufficient expiration. An attacker who obtains a valid token (for example via interception, log exposure, or token reuse on a shared system) can continue to authenticate to the management interface until the token is revoked, enabling unauthorized access to device functions and data.	N/A	More Details
CVE-2025-69252	free5gc UDM provides Unified Data Management (UDM) for free5GC, an open-source project for 5th generation (5G) mobile core networks. Versions up to and including 1.4.1 have a NULL Pointer Dereference vulnerability. Remote unauthenticated attackers can trigger a service panic (Denial of Service) by sending a crafted PUT request with an unexpected ueId, crashing the UDM service. All deployments of free5GC using the UDM component may be affected. free5gc/udm pull request 76 contains a fix for the issue. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2026-26341	Tattile Smart+, Vega, and Basic device families firmware versions 1.181.5 and prior ship with default credentials that are not forced to be changed during installation or commissioning. An attacker who can reach the management interface can authenticate using the default credentials and gain administrative access, enabling unauthorized access to device configuration and data.	N/A	More Details
CVE-2025-69251	free5gc UDM provides Unified Data Management (UDM) for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, remote attackers can inject control characters (e.g., %00) into the ueId parameter, triggering internal URL parsing errors (net/url: invalid control character). This exposes system implementation details and can aid in service fingerprinting. All deployments of free5GC using the UDM Nudm_UECM service may be affected. free5gc/udm pull request 76 contains a fix for the issue. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2026-3062	Out of bounds read and write in Tint in Google Chrome on Mac prior to 145.0.7632.116 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2025-69250	free5gc UDM provides Unified Data Management (UDM) for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, the service reliably leaks detailed internal error messages (e.g., strconv.ParseInt parsing errors) to remote clients when processing invalid pduSessionId inputs. This exposes implementation details and can be used for service fingerprinting. All deployments of free5GC using the UDM Nudm_UECM DELETE service may be vulnerable. free5gc/udm pull request 76 contains a fix for the issue. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2026-2459	A vulnerability exists in REB500 for an authenticated user with Installer role to access and alter the contents of directories that the role is not authorized to do so.	N/A	More Details
CVE-2026-2760	Sandbox escape due to incorrect boundary conditions in the Graphics: WebRender component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-3063	Inappropriate implementation in DevTools in Google Chrome prior to 145.0.7632.116 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via DevTools. (Chromium security severity: High)	N/A	More Details
CVE-2026-27195	Wasmtime is a runtime for WebAssembly. Starting with Wasmtime 39.0.0, the `component-model-async` feature became the default, which brought with it a new implementation of `[Typed]Func::call_async` which made it capable of calling async-typed guest export functions. However, that implementation had a bug leading to a panic under certain circumstances: First, the host embedding calls `[Typed]Func::call_async` on a function exported by a component, polling the returned `Future` once. Second, the component function yields control to the async runtime (e.g. Tokio), e.g. due to a call to host function registered using `LinkerInstance::func_wrap_async` which yields, or due an epoch interruption. Third, the host embedding drops the `Future` after polling it once. This leaves the component instance in a non-reenterable state since the call never had a chance to complete. Fourth, the host embedding calls `[Typed]Func::call_async` again, polling the returned `Future`. Since the component instance cannot be entered at this point, the call traps, but not before allocating a task and thread for the call. Fifth, the host embedding ignores the trap and drops the `Future`. This panics due to the runtime attempting to dispose of the task created above, which panics since the thread has not yet exited. When a host embedder using the affected versions of Wasmtime calls `wasmtime::component::[Typed]Func::call_async` on a guest export and then drops the returned future without waiting for it to resolve, and then does so again with the same component instance, Wasmtime will panic. Embeddings that have the `component-model-async` compile-time feature disabled are unaffected. Wasmtime 40.0.4 and 41.0.4 have been patched to fix this issue. Versions 42.0.0 and later are not affected. If an embedding is not actually using any component-model-async features then disabling the `component-model-async` Cargo feature can work around this issue. This issue can also be worked around by either ensuring every `call_async` future is awaited until it completes or refraining from using the `Store` again after dropping a not-yet-resolved `call_async` future.	N/A	More Details
CVE-2026-27033	Rejected reason: Not used	N/A	More Details

CVE-2025-69253	free5GC is an open-source project for 5th generation (5G) mobile core networks. Versions up to and including 1.4.1 of the User Data Repository are affected by Improper Error Handling with Information Exposure. The NEF component reliably leaks internal parsing error details (e.g., invalid character 'n' after top-level value) to remote clients, which can aid attackers in service fingerprinting. All deployments of free5GC using the Nnef_PfdManagement service may be vulnerable. free5gc/udr pull request 56 contains a patch. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2026-27204	Wasmtime is a runtime for WebAssembly. Prior to versions 24.0.6, 36.0.6, 4.0.04, 41.0.4, and 42.0.0, Wasmtime's implementation of WASI host interfaces are susceptible to guest-controlled resource exhaustion on the host. Wasmtime did not appropriately place limits on resource allocations requested by the guests. This serves as a Denial of Service vector. Wasmtime 24.0.6, 36.0.6, 40.0.4, 41.0.4, and 42.0.0 have all been released with the fix for this issue. These versions do not prevent this issue in their default configuration to avoid breaking preexisting behaviors. All versions of Wasmtime have appropriate knobs to prevent this behavior, and Wasmtime 42.0.0-and-later will have these knobs tuned by default to prevent this issue from happening. There are no known workarounds for this issue without upgrading. Embedders are recommended to upgrade and configure their embeddings as necessary to prevent possibly-malicious guests from triggering this issue.	N/A	More Details
CVE-2026-27034	Rejected reason: Not used	N/A	More Details
CVE-2026-23982	An Improper Authorization vulnerability exists in Apache Superset that allows a low-privileged user to bypass data access controls. When creating a dataset, Superset enforces permission checks to prevent users from querying unauthorized data. However, an authenticated attacker with permissions to write datasets and read charts can bypass these checks by overwriting the SQL query of an existing dataset. This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue.	N/A	More Details
CVE-2025-9120	Improper Control of Generation of Code ('Code Injection') vulnerability in OpenText™ Carbonite Safe Server Backup allows Code Injection. The vulnerability could be exploited through an open port, potentially allowing unauthorized access. This issue affects Carbonite Safe Server Backup: through 6.8.3.	N/A	More Details
CVE-2026-2761	Sandbox escape in the Graphics: WebRender component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-1773	IEC 60870-5-104: Potential Denial of Service impact on reception of invalid U-format frame. Product is only affected if IEC 60870-5-104 bi-directional functionality is configured. Enabling secure communication following IEC 62351-3 does not remediate the vulnerability but mitigates the risk of exploitation.	N/A	More Details
CVE-2026-2634	Malicious scripts could cause desynchronization between the address bar and web content before a response is received in Firefox iOS, allowing attacker-controlled pages to be presented under spoofed domains. This vulnerability affects Firefox for iOS < 147.4.	N/A	More Details
CVE-2026-2460	A vulnerability exists in REB500 for an authenticated user with low-level privileges to access and alter the content of directories by using the DAC protocol that the user is not authorized to do so.	N/A	More Details
CVE-2026-2762	Integer overflow in the JavaScript: Standard Library component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-25591	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to version 0.10.8-alpha.10, a SQL LIKE wildcard injection vulnerability in the `/api/token/search` endpoint allows authenticated users to cause denial of service through resource exhaustion by crafting malicious search patterns. The token search endpoint accepts user-supplied `keyword` and `token` parameters that are directly concatenated into SQL LIKE clauses without escaping wildcard characters (`%`, `_`). This allows attackers to inject patterns that trigger expensive database queries. Version 0.10.8-alpha.10 contains a patch.	N/A	More Details
CVE-2026-2799	Use-after-free in the DOM: Core & HTML component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2792	Memory safety bugs present in Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147 and Thunderbird 147. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2793	Memory safety bugs present in Firefox ESR 115.32, Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147 and Thunderbird 147. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2794	Information disclosure due to uninitialized memory in Firefox and Firefox Focus for Android. This vulnerability affects Firefox < 148.	N/A	More Details
CVE-2026-2795	Use-after-free in the JavaScript: GC component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2796	JIT miscompilation in the JavaScript: WebAssembly component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details

CVE-2026-2797	Use-after-free in the JavaScript: GC component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2776	Sandbox escape due to incorrect boundary conditions in the Telemetry component in External Software. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2800	Spoofing issue in the WebAuthn component in Firefox for Android. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2772	Use-after-free in the Audio/Video: Playback component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2801	Incorrect boundary conditions in the JavaScript: WebAssembly component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2775	Mitigation bypass in the DOM: HTML Parser component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2803	Information disclosure, mitigation bypass in the Settings UI component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2774	Integer overflow in the Audio/Video component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2773	Incorrect boundary conditions in the Web Audio component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2805	Invalid pointer in the DOM: Core & HTML component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2806	Uninitialized memory in the Graphics: Text component. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2026-2791	Mitigation bypass in the Networking: Cache component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2790	Same-origin policy bypass in the Networking: JAR component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2777	Privilege escalation in the Messaging System component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2789	Use-after-free in the Graphics: ImageLib component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-27128	Craft is a content management system (CMS). In versions 4.5.0-RC1 through 4.16.18 and 5.0.0-RC1 through 5.8.22, a Time-of-Check-Time-of-Use (TOCTOU) race condition exists in Craft CMS's token validation service for tokens that explicitly set a limited usage. The `getTokenRoute()` method reads a token's usage count, checks if it's within limits, then updates the database in separate non-atomic operations. By sending concurrent requests, an attacker can use a single-use impersonation token multiple times before the database update completes. To make this work, an attacker needs to obtain a valid user account impersonation URL with a non-expired token via some other means and exploit a race condition while bypassing any rate-limiting rules in place. For this to be a privilege escalation, the impersonation URL must include a token for a user account with more permissions than the current user. Versions 4.16.19 and 5.8.23 patch the issue.	N/A	More Details
CVE-2026-2781	Integer overflow in the Libraries component in NSS. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-27127	Craft is a content management system (CMS). In versions 4.5.0-RC1 through 4.16.18 and 5.0.0-RC1 through 5.8.22, the SSRF validation in Craft CMS's GraphQL Asset mutation performs DNS resolution separately from the HTTP request. This Time-of-Check-Time-of-Use (TOCTOU) vulnerability enables DNS rebinding attacks, where an attacker's DNS server returns different IP addresses for validation compared to the actual request. This is a bypass of the security fix for CVE-2025-68437 that allows access to all blocked IPs, not just IPv6 endpoints. Exploitation requires GraphQL schema permissions for editing assets in the `<VolumeName>` volume and creating assets in the `<VolumeName>` volume. These permissions may be granted to authenticated users with appropriate GraphQL schema access and/or Public Schema (if misconfigured with write permissions). Versions 4.16.19 and 5.8.23 patch the issue.	N/A	More Details
	Craft is a content management system (CMS). In versions 4.5.0-RC1 through 4.16.18 and 5.0.0-RC1 through 5.8.22, a stored		

CVE-2026-27126	Cross-site Scripting (XSS) vulnerability exists in the `editableTable.twig` component when using the `html` column type. The application fails to sanitize the input, allowing an attacker to execute arbitrary JavaScript when another user views a page with the malicious table field. In order to exploit the vulnerability, an attacker must have an administrator account, and `allowAdminChanges` must be enabled in production, which is against Craft's security recommendations. Versions 4.16.19 and 5.8.23 patch the issue.	N/A	More Details
CVE-2026-2782	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-27461	Pimcore is an Open Source Data & Experience Management Platform. In versions up to and including 11.5.14.1 and 12.3.2, the filter query parameter in the dependency listing endpoints is JSON-decoded and the value field is concatenated directly into RLIKE clauses without sanitization or parameterized queries. Exploiting this issue requires admin authentication. An attacker with admin panel access can extract the full database including password hashes of other admin users. Version 12.3.3 contains a patch.	N/A	More Details
CVE-2026-2783	Information disclosure due to JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2784	Mitigation bypass in the DOM: Security component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2785	Invalid pointer in the JavaScript Engine component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2780	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2779	Incorrect boundary conditions in the Networking: JAR component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2786	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2787	Use-after-free in the DOM: Window and Location component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2788	Incorrect boundary conditions in the Audio/Video: GMP component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2778	Sandbox escape due to incorrect boundary conditions in the DOM: Core & HTML component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2807	Memory safety bugs present in Firefox 147 and Thunderbird 147. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 148 and Thunderbird < 148.	N/A	More Details
CVE-2025-67445	TOTOLINK X5000R V9.1.0cu.2415_B20250515 contains a denial-of-service vulnerability in /cgi-bin/cstecgi.cgi. The CGI reads the CONTENT_LENGTH environment variable and allocates memory using malloc (CONTENT_LENGTH + 1) without sufficient bounds checking. When lighttpd s request size limit is not enforced, a crafted large POST request can cause memory exhaustion or a segmentation fault, leading to a crash of the management CGI and loss of availability of the web interface.	N/A	More Details
CVE-2025-14577	Slican NCP/IPL/IPM/IPU devices are vulnerable to PHP Function Injection. An unauthenticated remote attacker is able to execute arbitrary PHP commands by sending specially crafted requests to /webcti/session_ajax.php endpoint. This issue was fixed in version 1.24.0190 (Slican NCP) and 6.61.0010 (Slican IPL/IPM/IPU).	N/A	More Details
CVE-2026-25421	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. Collision with another CVE.	N/A	More Details
CVE-2026-27586	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, two swallowed errors in `ClientAuthentication.provision()` cause mTLS client certificate authentication to silently fail open when a CA certificate file is missing, unreadable, or malformed. The server starts without error but accepts any client certificate signed by any system-trusted CA, completely bypassing the intended private CA trust boundary. Any deployment using `trusted_ca_cert_file` or `trusted_ca_certs_pem_files` for mTLS will silently degrade to accepting any system-trusted client certificate if the CA file becomes unavailable. This can happen due to a typo in the path, file rotation, corruption, or permission changes. The server gives no indication that mTLS is misconfigured. Version 2.11.1 fixes the vulnerability.	N/A	More Details
CVE-2026-27643	free5GC UDR is the user data repository (UDR) for free5GC, an an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, the NEF component reliably leaks internal parsing error details (e.g., invalid character 'n' after top-level value) to remote clients, which can aid attackers in service fingerprinting. All deployments of free5GC using the Nnef_PfdManagement service may be affected. free5gc/udr pull request 56 contains a patch for the issue. There is no direct workaround at the application level. The recommendation is to apply the provided patch.	N/A	More Details

CVE-2026-27642	free5gc UDM provides Unified Data Management (UDM) for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, remote attackers can inject control characters (e.g., %00) into the supi parameter, triggering internal URL parsing errors (net/url: invalid control character). This exposes system-level error details and can be used for service fingerprinting. All deployments of free5GC using the UDM Nudm_UEAU service may be affected. free5gc/udm pull request 75 contains a fix for the issue. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2026-26025	free5GC SMF provides Session Management Function for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, SMF panics and terminates when processing a malformed PFCP SessionReportRequest on the PFCP (UDP/8805) interface. No known upstream fix is available, but some workarounds are available. ACL/firewall the PFCP interface so only trusted UPF IPs can reach SMF (reduce spoofing/abuse surface); drop/inspect malformed PFCP SessionReportRequest messages at the network edge where feasible, and/or add recover() around PFCP handler dispatch to avoid whole-process termination (mitigation only).	N/A	More Details
CVE-2026-26024	free5GC SMF provides Session Management Function for free5GC, an open-source project for 5th generation (5G) mobile core networks. In versions up to and including 1.4.1, SMF panics and terminates when processing a malformed PFCP SessionReportRequest on the PFCP (UDP/8805) interface. No known upstream fix is available, but some workarounds are available. ACL/firewall the PFCP interface so only trusted UPF IPs can reach SMF (reduce spoofing/abuse surface); drop/inspect malformed PFCP SessionReportRequest messages at the network edge where feasible, and/or add recover() around PFCP handler dispatch to avoid whole-process termination (mitigation only).	N/A	More Details
CVE-2026-27587	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, Caddy's HTTP `path` request matcher is intended to be case-insensitive, but when the match pattern contains percent-escape sequences (`%xx`) it compares against the request's escaped path without lowercasing. An attacker can bypass path-based routing and any access controls attached to that route by changing the casing of the request path. Version 2.11.1 contains a fix for the issue.	N/A	More Details
CVE-2026-27588	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, Caddy's HTTP `host` request matcher is documented as case-insensitive, but when configured with a large host list (>100 entries) it becomes case-sensitive due to an optimized matching path. An attacker can bypass host-based routing and any access controls attached to that route by changing the casing of the `Host` header. Version 2.11.1 contains a fix for the issue.	N/A	More Details
CVE-2026-27589	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, the local caddy admin API (default listen `127.0.0.1:2019`) exposes a state-changing `POST /load` endpoint that replaces the entire running configuration. When origin enforcement is not enabled (`enforce_origin` not configured), the admin endpoint accepts cross-origin requests (e.g., from attacker-controlled web content in a victim browser) and applies an attacker-supplied JSON config. This can change the admin listener settings and alter HTTP server behavior without user intent. Version 2.11.1 contains a fix for the issue.	N/A	More Details
CVE-2026-2771	Undefined behavior in the DOM: Core & HTML component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-27590	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, Caddy's FastCGI path splitting logic computes the split index on a lowercased copy of the request path and then uses that byte index to slice the original path. This is unsafe for Unicode because `strings.ToLower()` can change UTF-8 byte length for some characters. As a result, Caddy can derive an incorrect `SCRIPT_NAME`/`SCRIPT_FILENAME` and `PATH_INFO`, potentially causing a request that contains `.php` to execute a different on-disk file than intended (path confusion). In setups where an attacker can control file contents (e.g., upload features), this can lead to unintended PHP execution of non-.php files (potential RCE depending on deployment). Version 2.11.1 fixes the issue.	N/A	More Details
CVE-2025-14963	A vulnerability identified in the Trellix HX Agent driver file fekern.sys allowed a threat actor with local user access the ability to gain elevated system privileges. Utilization of a Bring Your Own Vulnerable Driver (BYOVD) was leveraged to gain access to the critical Windows process memory lsass.exe (Local Security Authority Subsystem Service). The fekern.sys; a driver file associated with Trellix HX Agent (used in all existing HX Agent versions). The vulnerable driver installed in a product or a system running fully functional HX Agent is, itself, not exploitable as the product’s tamper protection restricts the ability to communicate with the driver to only the agent’s processes.	N/A	More Details
CVE-2025-62512	Piwigo is an open source photo gallery application for the web. In version 15.5.0 and likely earlier 15.x releases, the password reset functionality in Piwigo allows an unauthenticated attacker to determine whether a given username or email address exists in the system. The endpoint at password.php?action=lost returns distinct messages for valid vs. invalid accounts, enabling user enumeration. As of time of publication, no known patches are available.	N/A	More Details
CVE-2026-27038	Rejected reason: Not used	N/A	More Details
CVE-2026-26222	Altec DocLink (now maintained by Beyond Limits Inc.) version 4.0.336.0 exposes insecure .NET Remoting endpoints over TCP and HTTP/SOAP via Altec.RDCHostService.exe using the ObjectURI "doclinkServer.soap". The service does not require authentication and is vulnerable to unsafe object unmarshalling, allowing remote attackers to read arbitrary files from the underlying system by specifying local file paths. Additionally, attackers can coerce SMB authentication via UNC paths and write arbitrary files to server locations. Because writable paths may be web-accessible under IIS, this can result in unauthenticated remote code execution or denial of service through file overwrite.	N/A	More Details
CVE-2026-27468	Mastodon is a free, open-source social network server based on ActivityPub. FASP registration requires manual approval by an administrator. In versions 4.4.0 through 4.4.13 and 4.5.0 through 4.5.6, actions performed by a FASP to subscribe to account/content lifecycle events or to backfill content did not check properly whether the FASP was actually approved. This only affects Mastodon servers that have opted in to testing the experimental FASP feature by setting the environment variable `EXPERIMENTAL_FEATURES` to a value including `fasp`. An attacker can make subscriptions and request content backfill without approval by an administrator. Done once, this leads to minor information leak of URIs that are publicly available anyway. But done several times this is a serious vector for DOS, putting pressure on the sidekiq worker responsible for the `fasp` queue. The fix is included in the 4.4.14 and 4.5.7 releases. Admins that are actively testing the experimental "fasp" feature should update their systems. Servers not using the experimental feature flag `fasp` are not affected.	N/A	More Details

CVE-2026-2664	An out of bounds read vulnerability in the grpcfuse kernel module present in the Linux VM in Docker Desktop for Windows, Linux and macOS up to version 4.61.0 could allow a local attacker to cause an unspecified impact by writing to /proc/docker entries. The issue has been fixed in Docker Desktop 4.62.0 .	N/A	More Details
CVE-2026-27585	Caddy is an extensible server platform that uses TLS by default. Prior to version 2.11.1, the path sanitization routine in file matcher doesn't sanitize backslashes which can lead to bypassing path related security protections. It affects users with specific Caddy and environment configurations. Version 2.11.1 fixes the issue.	N/A	More Details
CVE-2025-13776	Multiple Finka programs use hard-coded Firebird database credentials (shared across all instances of this software). A malicious attacker in local network who knows default credentials is able to read and edit database content. This vulnerability has been fixed in version: Finka-FK 18.5, Finka-KPR 16.6, Finka-Płace 13.4, Finka-Faktura 18.3, Finka-Magazyn 8.3, Finka-STW 12.3	N/A	More Details
CVE-2024-48928	Piwigo is an open source photo gallery application for the web. In versions on the 14.x branch, when installing, the secret_key configuration parameter is set to MD5(RAND()) in MySQL. However, RAND() only has 30 bits of randomness, making it feasible to brute-force the secret key. The CSRF token is constructed partially from the secret key, and this can be used to check if the brute force succeeded. Trying all possible values takes approximately one hour. The impact of this is limited. The auto login key uses the user's password on top of the secret key. The pwg token uses the user's session identifier on top of the secret key. It seems that values for get_ephemeral_key can be generated when one knows the secret key. Version 15.0.0 contains a fix for the issue.	N/A	More Details
CVE-2026-27129	Craft is a content management system (CMS). In versions 4.5.0-RC1 through 4.16.18 and 5.0.0-RC1 through 5.8.22, the SSRF validation in Craft CMS's GraphQL Asset mutation uses `gethostbyname()`, which only resolves IPv4 addresses. When a hostname has only AAAA (IPv6) records, the function returns the hostname string itself, causing the blocklist comparison to always fail and completely bypassing SSRF protection. This is a bypass of the security fix for CVE-2025-68437. Exploitation requires GraphQL schema permissions for editing assets in the `<VolumeName>` volume and creating assets in the `<VolumeName>` volume. These permissions may be granted to authenticated users with appropriate GraphQL schema access and/or Public Schema (if misconfigured with write permissions). Versions 4.16.19 and 5.8.23 patch the issue.	N/A	More Details
CVE-2026-2770	Use-after-free in the DOM: Bindings (WebIDL) component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2768	Sandbox escape in the Storage: IndexedDB component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2767	Use-after-free in the JavaScript: WebAssembly component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-2766	Use-after-free in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-27568	WWBN AVideo is an open source video platform. Prior to version 21.0, AVideo allows Markdown in video comments and uses Parsedown (v1.7.4) without Safe Mode enabled. Markdown links are not sufficiently sanitized, allowing `javascript:` URIs to be rendered as clickable links. An authenticated low-privilege attacker can post a malicious comment that injects persistent JavaScript. When another user clicks the link, the attacker can perform actions such as session hijacking, privilege escalation (including admin takeover), and data exfiltration. Version 21.0 contains a fix. As a workaround, validate and block unsafe URI schemes (e.g., `javascript:`) before rendering Markdown, and enable Parsedown Safe Mode.	N/A	More Details
CVE-2026-27584	Actual is a local-first personal finance tool. Prior to version 26.2.1, missing authentication middleware in the ActualBudget server component allows any unauthenticated user to query the SimpleFIN and Pluggy.ai integration endpoints and read sensitive bank account balance and transaction information. This vulnerability allows an unauthenticated attacker to read the bank account balance and transaction history of ActualBudget users. This vulnerability impacts all ActualBudget Server users with the SimpleFIN or Pluggy.ai integrations configured. The ActualBudget Server instance must be reachable over the network. Version 26.2.1 patches the issue.	N/A	More Details
CVE-2026-27732	WWBN AVideo is an open source video platform. Prior to version 22.0, the `aVideoEncoder.json.php` API endpoint accepts a `downloadURL` parameter and fetches the referenced resource server-side without proper validation or an allow-list. This allows authenticated users to trigger server-side requests to arbitrary URLs (including internal network endpoints). An authenticated attacker can leverage SSRF to interact with internal services and retrieve sensitive data (e.g., internal APIs, metadata services), potentially leading to further compromise depending on the deployment environment. This issue has been fixed in AVideo version 22.0.	N/A	More Details
CVE-2026-2765	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 148, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2026-1229	The CombinedMult function in the CIRCL ecc/p384 package (secp384r1 curve) produces an incorrect value for specific inputs. The issue is fixed by using complete addition formulas. ECDH and ECDSA signing relying on this curve are not affected. The bug was fixed in v1.6.3 https://github.com/cloudflare/circl/releases/tag/v1.6.3 .	N/A	More Details
CVE-2025-47904	Download of Code Without Integrity Check vulnerability in Microchip Time Provider 4100 allows Malicious Manual Software Update.This issue affects Time Provider 4100: before 2.5.	N/A	More Details
CVE-2026-2764	JIT miscompilation, use-after-free in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-	Privilege escalation and improper access control in GCOM EPON 1GE C00R371V00B01 allows remote authenticated users to		More

2025-63409	modify administrator only settings and extract administrator credentials.	N/A	Details
CVE-2025-69985	FUXA 1.2.8 and prior contains an Authentication Bypass vulnerability leading to Remote Code Execution (RCE). The vulnerability exists in the server/api/jwt-helper.js middleware, which improperly trusts the HTTP "Referer" header to validate internal requests. A remote unauthenticated attacker can bypass JWT authentication by spoofing the Referer header to match the server's host. Successful exploitation allows the attacker to access the protected /api/runscript endpoint and execute arbitrary Node.js code on the server.	N/A	More Details
CVE-2026-2763	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2025-11165	A sandbox escape vulnerability exists in dotCMS’s Velocity scripting engine (VTools) that allows authenticated users with scripting privileges to bypass class and package restrictions enforced by SecureUberspectorImpl. By dynamically modifying the Velocity engine’s runtime configuration and reinitializing its Uberspect, a malicious actor can remove the introspector.restrict.classes and introspector.restrict.packages protections. Once these restrictions are cleared, the attacker can access arbitrary Java classes, including java.lang.Runtime, and execute arbitrary system commands under the privileges of the application process (e.g. dotCMS or Tomcat user).	N/A	More Details
CVE-2026-2758	Use-after-free in the JavaScript: GC component. This vulnerability affects Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8.	N/A	More Details
CVE-2025-71249	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-27163	Rejected reason: This CVE was assigned in error.	N/A	More Details
CVE-2025-68042	Missing Authorization vulnerability in Travelpayouts Travelpayouts travelpayouts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travelpayouts: from n/a through <= 1.2.1.	N/A	More Details
CVE-2025-68837	Missing Authorization vulnerability in ELEXtensions ELEX WordPress HelpDesk & Customer Ticketing System elex-helpdesk-customer-support-ticket-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ELEX WordPress HelpDesk & Customer Ticketing System: from n/a through <= 3.3.5.	N/A	More Details
CVE-2025-68834	Missing Authorization vulnerability in Saiful Islam Sync Master Sheet – Product Sync with Google Sheet for WooCommerce product-sync-master-sheet allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sync Master Sheet – Product Sync with Google Sheet for WooCommerce: from n/a through <= 1.1.3.	N/A	More Details
CVE-2025-68564	Missing Authorization vulnerability in sendy Sendy sendy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sendy: from n/a through <= 3.4.2.	N/A	More Details
CVE-2025-68552	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WebCodingPlace WooCommerce Coming Soon Product with Countdown woo-coming-soon-product allows PHP Local File Inclusion.This issue affects WooCommerce Coming Soon Product with Countdown: from n/a through <= 5.0.	N/A	More Details
CVE-2025-68549	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Wiguard wiguard allows Upload a Web Shell to a Web Server.This issue affects Wiguard: from n/a through < 2.0.1.	N/A	More Details
CVE-2025-68545	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Nika nika allows PHP Local File Inclusion.This issue affects Nika: from n/a through <= 1.2.14.	N/A	More Details
CVE-2026-25387	Missing Authorization vulnerability in Elementor Image Optimizer by Elementor image-optimization allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Optimizer by Elementor: from n/a through <= 1.7.1.	N/A	More Details
CVE-2025-68514	Authorization Bypass Through User-Controlled Key vulnerability in Cozmoslabs Paid Member Subscriptions paid-member-subscriptions allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Paid Member Subscriptions: from n/a through <= 2.16.8.	N/A	More Details
CVE-2026-25389	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Retrieve Embedded Sensitive Data.This issue affects EventPrime: from n/a through <= 4.2.8.3.	N/A	More Details
CVE-2025-68051	Authorization Bypass Through User-Controlled Key vulnerability in Shiprocket Shiprocket shiprocket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Shiprocket: from n/a through <= 2.0.8.	N/A	More Details
CVE-2025-68048	Missing Authorization vulnerability in XLPlugins NextMove Lite woo-thank-you-page-nextmove-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects NextMove Lite: from n/a through <= 2.23.0.	N/A	More Details
CVE-2025-68032	Missing Authorization vulnerability in Passionate Brains Advanced WC Analytics advance-wc-analytics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced WC Analytics: from n/a through <= 3.19.0.	N/A	More Details

CVE-2026-25363	Missing Authorization vulnerability in FooPlugins FooGallery foogallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FooGallery: from n/a through <= 3.1.11.	N/A	More Details
CVE-2025-68028	Missing Authorization vulnerability in Passionate Brains GA4WP: Google Analytics for WordPress ga-for-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GA4WP: Google Analytics for WordPress: from n/a through <= 2.10.0.	N/A	More Details
CVE-2025-68025	Missing Authorization vulnerability in Addonify Addonify Floating Cart For WooCommerce addonify-floating-cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Addonify Floating Cart For WooCommerce: from n/a through <= 1.2.17.	N/A	More Details
CVE-2025-68023	Missing Authorization vulnerability in Addonify Addonify – Compare Products For WooCommerce addonify-compare-products allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Addonify – Compare Products For WooCommerce: from n/a through <= 1.1.17.	N/A	More Details
CVE-2025-68021	Missing Authorization vulnerability in ConveyThis ConveyThis conveythis-translate allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ConveyThis: from n/a through <= 269.5.	N/A	More Details
CVE-2025-68002	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in 100plugins Open User Map open-user-map allows Path Traversal.This issue affects Open User Map: from n/a through <= 1.4.16.	N/A	More Details
CVE-2025-67998	Authentication Bypass Using an Alternate Path or Channel vulnerability in kamleshyadav Miraculous Elementor miraculous-el allows Authentication Abuse.This issue affects Miraculous Elementor: from n/a through <= 2.0.7.	N/A	More Details
CVE-2025-67994	Missing Authorization vulnerability in YayCommerce YayCurrency yaycurrency allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YayCurrency: from n/a through <= 3.3.	N/A	More Details
CVE-2026-25412	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-25422	Cross-Site Request Forgery (CSRF) vulnerability in Themes4WP Popularis Extra popularis-extra allows Cross Site Request Forgery.This issue affects Popularis Extra: from n/a through <= 1.2.10.	N/A	More Details
CVE-2025-67979	Improper Control of Generation of Code ('Code Injection') vulnerability in WesternDeal WPForms Google Sheet Connector gsheetconnector-wpforms allows Code Injection.This issue affects WPForms Google Sheet Connector: from n/a through <= 4.0.1.	N/A	More Details
CVE-2025-67975	Missing Authorization vulnerability in aDirectory aDirectory adirectory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects aDirectory: from n/a through <= 3.0.3.	N/A	More Details
CVE-2026-25370	Missing Authorization vulnerability in AresIT WP Compress wp-compress-image-optimizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Compress: from n/a through <= 6.60.28.	N/A	More Details
CVE-2025-68855	Insertion of Sensitive Information Into Sent Data vulnerability in themeglow JobBoard Job listing job-board-light allows Retrieve Embedded Sensitive Data.This issue affects JobBoard Job listing: from n/a through <= 1.2.8.	N/A	More Details
CVE-2025-67969	Missing Authorization vulnerability in knitpay UPI QR Code Payment Gateway for WooCommerce upi-qr-code-payment-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UPI QR Code Payment Gateway for WooCommerce: from n/a through <= 1.5.1.	N/A	More Details
CVE-2026-25305	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore xstore allows DOM-Based XSS.This issue affects XStore: from n/a through <= 9.6.4.	N/A	More Details
CVE-2025-40697	Reflected Cross-Site Scripting (XSS) vulnerability in '/index.php' in Lewe WebMeasure, which allows remote attackers to execute arbitrary code through the 'page' parameter. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-41023	An authentication bypass vulnerability has been found in Thesamur's AutoGPT. This vulnerability allows an attacker to bypass authentication mechanisms. Once inside the web application, the attacker can use any of its features regardless of the authorisation method used.	N/A	More Details
CVE-2025-69403	Unrestricted Upload of File with Dangerous Type vulnerability in Bravis-Themes Bravis Addons bravis-addons allows Using Malicious Files.This issue affects Bravis Addons: from n/a through <= 1.1.9.	N/A	More Details
CVE-2025-69401	Authentication Bypass by Spoofing vulnerability in mdalabar WooODT Lite byconsole-woo-order-delivery-time allows Identity Spoofing.This issue affects WooODT Lite: from n/a through <= 2.5.2.	N/A	More Details
CVE-2026-	Missing Authorization vulnerability in WPFunnels Mail Mint mail-mint allows Accessing Functionality Not Properly Constrained by	N/A	More

23541	ACLs.This issue affects Mail Mint: from n/a through <= 1.19.4.		Details
CVE-2026-23543	Missing Authorization vulnerability in WPDeveloper Essential Addons for Elementor essential-addons-for-elementor-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Essential Addons for Elementor: from n/a through <= 6.5.5.	N/A	More Details
CVE-2026-23545	Missing Authorization vulnerability in Aruba.it Dev Aruba HiSpeed Cache aruba-hispeed-cache allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Aruba HiSpeed Cache: from n/a through <= 3.0.4.	N/A	More Details
CVE-2026-23548	Missing Authorization vulnerability in designinvento DirectoryPress directorypress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DirectoryPress: from n/a through <= 3.6.25.	N/A	More Details
CVE-2025-69394	Authorization Bypass Through User-Controlled Key vulnerability in cnvrse Cnvrse cnvrse allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cnvrse: from n/a through <= 026.02.10.20.	N/A	More Details
CVE-2026-25004	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Business Directory cm-business-directory allows Stored XSS.This issue affects CM Business Directory: from n/a through <= 1.5.3.	N/A	More Details
CVE-2026-25006	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in 8theme XStore xstore allows Code Injection.This issue affects XStore: from n/a through <= 9.6.4.	N/A	More Details
CVE-2025-69381	Missing Authorization vulnerability in vanquish WooCommerce Bulk Product Editor woocommerce-quick-product-editor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Bulk Product Editor: from n/a through <= 3.0.	N/A	More Details
CVE-2025-68862	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Murtaza Bhurgri Woo File Dropzone woo-file-dropzone allows Path Traversal.This issue affects Woo File Dropzone: from n/a through <= 1.1.7.	N/A	More Details
CVE-2025-69379	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vanquish Upload Files Anywhere wp-upload-files-anywhere allows Path Traversal.This issue affects Upload Files Anywhere: from n/a through <= 2.8.	N/A	More Details
CVE-2025-69378	Incorrect Privilege Assignment vulnerability in XforWooCommerce Product Filter for WooCommerce prdctfltr allows Privilege Escalation.This issue affects Product Filter for WooCommerce: from n/a through <= 9.1.2.	N/A	More Details
CVE-2025-69377	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vanquish User Extra Fields wp-user-extra-fields allows Path Traversal.This issue affects User Extra Fields: from n/a through <= 17.0.	N/A	More Details
CVE-2025-69376	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vanquish User Extra Fields wp-user-extra-fields allows Path Traversal.This issue affects User Extra Fields: from n/a through <= 17.0.	N/A	More Details
CVE-2025-69303	Missing Authorization vulnerability in modeltheme ModelTheme Framework modeltheme-framework allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ModelTheme Framework: from n/a through <= 1.9.2.	N/A	More Details
CVE-2026-25323	Missing Authorization vulnerability in MiKa OSM osm allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects OSM: from n/a through <= 6.1.12.	N/A	More Details
CVE-2025-69298	Missing Authorization vulnerability in GhostPool Gauge gauge allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gauge: from n/a through <= 6.56.4.	N/A	More Details
CVE-2026-25329	Missing Authorization vulnerability in ExpressTech Systems 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 <= 10.3.4.	N/A	More Details
CVE-2026-25331	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Melapress WP Activity Log wp-security-audit-log allows DOM-Based XSS.This issue affects WP Activity Log: from n/a through <= 5.5.4.	N/A	More Details
CVE-2025-69011	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPKube Cool Tag Cloud cool-tag-cloud allows Stored XSS.This issue affects Cool Tag Cloud: from n/a through <= 2.29.	N/A	More Details
CVE-2025-68895	Authentication Bypass Using an Alternate Path or Channel vulnerability in ahachat AhaChat Messenger Marketing ahachat-messenger-marketing allows Password Recovery Exploitation.This issue affects AhaChat Messenger Marketing: from n/a through <= 1.1.	N/A	More Details
CVE-2025-67973	Missing Authorization vulnerability in sunshinephotocart Sunshine Photo Cart sunshine-photo-cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through <= 3.5.6.2.	N/A	More Details
CVE-			

2025-67547	Missing Authorization vulnerability in uixthemes Konte konte allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Konte: from n/a through <= 2.4.6.	N/A	More Details
CVE-2026-22350	Missing Authorization vulnerability in add-ons.org PDF for Elementor Forms + Drag And Drop Template Builder pdf-for-elementor-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PDF for Elementor Forms + Drag And Drop Template Builder: from n/a through <= 6.3.1.	N/A	More Details
CVE-2026-2738	Buffer overflow in ovpn-dco-win version 2.8.0 allows local attackers to cause a system crash by sending too large packets to the remote peer when the AEAD tag appears at the end of the encrypted packet	N/A	More Details
CVE-2025-30416	Sensitive data disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 39938, Acronis Cyber Protect 15 (Linux, Windows) before build 41800.	N/A	More Details
CVE-2025-30412	Sensitive data disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 39938, Acronis Cyber Protect 15 (Linux, Windows) before build 41800.	N/A	More Details
CVE-2025-30411	Sensitive data disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 39938, Acronis Cyber Protect 15 (Linux, Windows) before build 41800.	N/A	More Details
CVE-2025-30410	Sensitive data disclosure and manipulation due to missing authentication. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 39870, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 39938, Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 41800.	N/A	More Details
CVE-2026-26957	Libredesk is a self-hosted customer support desk application. Versions prior to 1.0.2-0.20260215211005-727213631ce6 fail to validate destination URLs for webhooks, allowing an attacker posing as an authenticated "Application Admin" to force the server to make HTTP requests to arbitrary internal destinations. This could compromise the underlying cloud infrastructure or internal corporate network where the service is hosted. This issue has been fixed in version 1.0.2-0.20260215211005-727213631ce6.	N/A	More Details
CVE-2026-26958	filippo.io/edwards25519 is a Go library implementing the edwards25519 elliptic curve with APIs for building cryptographic primitives. In versions 1.1.0 and earlier, MultiScalarMult produces invalid results or undefined behavior if the receiver is not the identity point. If (*Point).MultiScalarMult is called on an initialized point that is not the identity point, it returns an incorrect result. If the method is called on an uninitialized point, the behavior is undefined. In particular, if the receiver is the zero value, MultiScalarMult returns an invalid point that compares Equal to every other point. Note that MultiScalarMult is a rarely used, advanced API. For example, users who depend on filippo.io/edwards25519 only through github.com/go-sql-driver/mysql are not affected. This issue has been fixed in version 1.1.1.	N/A	More Details
CVE-2026-1658	User Interface (UI) Misrepresentation of Critical Information vulnerability in OpenText™ Directory Services allows Cache Poisoning. The vulnerability could be exploited by a bad actor to inject manipulated text into the OpenText application, potentially misleading users. This issue affects Directory Services: from 20.4.1 through 25.2.	N/A	More Details
CVE-2025-9208	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText™ Web Site Management Server allows Stored XSS. The vulnerability could execute malicious scripts on the client side when the download query parameter is removed from the file URL, allowing attackers to compromise user sessions and data. This issue affects Web Site Management Server: 16.7.X, 16.8, 16.8.1.	N/A	More Details
CVE-2025-8054	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText™ XM Fax allows Path Traversal. The vulnerability could allow an attacker to arbitrarily disclose content of files on the local filesystem. This issue affects XM Fax: 24.2.	N/A	More Details
CVE-2025-13672	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText™ Web Site Management Server allows Reflected XSS. The vulnerability could allow injecting malicious JavaScript inside URL parameters that was then rendered with the preview of the page, so that malicious scripts could be executed on the client side. This issue affects Web Site Management Server: 16.7.0, 16.7.1.	N/A	More Details
CVE-2025-13671	Cross-Site Request Forgery (CSRF) vulnerability in OpenText™ Web Site Management Server allows Cross Site Request Forgery. The vulnerability could make a user, with active session inside the product, click on a page that contains this malicious HTML triggering to perform changes unconsciously. This issue affects Web Site Management Server: 16.7.0, 16.7.1.	N/A	More Details
CVE-2026-27327	Missing Authorization vulnerability in YayCommerce YayMail – WooCommerce Email Customizer yaymail allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YayMail – WooCommerce Email Customizer: from n/a through <= 4.3.2.	N/A	More Details
CVE-2026-27074	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vaakash Shortcoder shortcoder allows Stored XSS.This issue affects Shortcoder: from n/a through <= 6.5.1.	N/A	More Details
CVE-2026-26205	opa-envoy-plugun is a plugin to enforce OPA policies with Envoy. Versions prior to 1.13.2-envoy-2 have a vulnerability in how the `input.parsed_path` field is constructed. HTTP request paths are treated as full URIs when parsed; interpreting leading path segments prefixed with double slashes (`//`) as authority components, and therefore dropping them from the parsed path. This creates a path interpretation mismatch between authorization policies and backend servers, enabling attackers to bypass access controls by crafting requests where the authorization filter evaluates a different path than the one ultimately served. Version 1.13.2-envoy-2 fixes the issue.	N/A	More Details
CVE-2026-26201	emp3r0r is a C2 designed by Linux users for Linux environments. Prior to version 3.21.2, multiple shared maps are accessed without consistent synchronization across goroutines. Under concurrent activity, Go runtime can trigger `fatal error: concurrent map read and map write`, causing C2 process crash (availability loss). Version 3.21.2 fixes this issue.	N/A	More Details

CVE-2026-26063	CediPay is a crypto-to-fiat app for the Ghanaian market. A vulnerability in CediPay prior to version 1.2.3 allows attackers to bypass input validation in the transaction API. The issue has been fixed in version 1.2.3. If upgrading is not immediately possible, restrict API access to trusted networks or IP ranges; enforce strict input validation at the application layer; and/or monitor transaction logs for anomalies or suspicious activity. These mitigations reduce exposure but do not fully eliminate the vulnerability.	N/A	More Details
CVE-2026-2744	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-2409	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Delinea Cloud Suite allows Argument Injection.This issue affects Cloud Suite: before 25.2 HF1.	N/A	More Details
CVE-2025-71245	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-71246	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-71247	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-2274	A SSRF and Arbitrary File Read vulnerability in AppSheet Core in Google AppSheet prior to 2025-11-23 allows an authenticated remote attacker to read sensitive local files and access internal network resources via crafted requests to the production cluster. This vulnerability was patched and no customer action is needed.	N/A	More Details
CVE-2025-71248	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-25738	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Versions prior to 3.3.10 are vulnerable to server-side request forgery. Indico makes outgoing requests to user-provides URLs in various places. This is mostly intentional and part of Indico's functionality but is never intended to let users access "special" targets such as localhost or cloud metadata endpoints. Users should upgrade to version 3.3.10 to receive a patch. Those who do not have IPs that expose sensitive data without authentication (typically because they do not host Indico on AWS) are not affected. Only event organizers can access endpoints where SSRF could be used to actually see the data returned by such a request. For those who trust their event organizers, the risk is also very limited. For additional security, both before and after patching, one may also use the common proxy-related environment variables (in particular `http_proxy` and `https_proxy`) to force outgoing requests to go through a proxy that limits requests in whatever way you deem useful/necessary. These environment variables would need to be set both on the indico-uwsgi and indico-celery services.	N/A	More Details
CVE-2026-26974	Slyde is a program that creates animated presentations from XML. In versions 0.0.4 and below, Node.js automatically imports **/*.plugin.{js,mjs} files including those from node_modules, so any malicious package with a .plugin.js file can execute arbitrary code when installed or required. All projects using this loading behavior are affected, especially those installing untrusted packages. This issue has been fixed in version 0.0.5. To workaround this issue, users can audit and restrict which packages are installed in node_modules.	N/A	More Details
CVE-2026-26995	Rejected reason: Further research determined the issue is an external dependency vulnerability.	N/A	More Details
CVE-2025-60183	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in silence Silencesoft RSS Reader external-rss-reader allows Stored XSS.This issue affects Silencesoft RSS Reader: from n/a through <= 0.6.	N/A	More Details
CVE-2025-14547	An integer underflow vulnerability is present in Silicon Lab’s implementation of PSA Crypto and SE Manager EC-JPAKE APIs during ZKP parsing. Triggering the underflow can lead to a hard fault, causing a temporary denial of service.	N/A	More Details
CVE-2025-53217	Missing Authorization vulnerability in staviravn AIO WP Builder all-in-one-wp-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AIO WP Builder: from n/a through <= 2.0.2.	N/A	More Details
CVE-2025-52744	Improper Control of Generation of Code ('Code Injection') vulnerability in inpersttion Inpersttion For Theme err-our-team allows Code Injection.This issue affects Inpersttion For Theme: from n/a through <= 1.0.	N/A	More Details
CVE-2024-56208	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in desertthemes NewsMash newsmash allows Stored XSS.This issue affects NewsMash: from n/a through <= 1.0.71.	N/A	More Details
CVE-2024-54222	Missing Authorization vulnerability in Seraphinite Solutions Seraphinite Accelerator seraphinite-accelerator allows Retrieve Embedded Sensitive Data.This issue affects Seraphinite Accelerator: from n/a through <= 2.22.15.	N/A	More Details
CVE-2024-52387	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liton Arefin Master Addons for Elementor master-addons allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through <= 2.0.9.9.4.	N/A	More Details

CVE-2024-51915	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache litespeed-cache allows Stored XSS.This issue affects LiteSpeed Cache: from n/a through <= 6.5.2.	N/A	More Details
CVE-2024-50555	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows Stored XSS.This issue affects Elementor Website Builder: from n/a through <= 3.29.0.	N/A	More Details
CVE-2024-50452	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POSIMYTH Nexter Blocks the-plus-addons-for-block-editor allows Stored XSS.This issue affects Nexter Blocks: from n/a through <= 3.3.3.	N/A	More Details
CVE-2024-43228	Missing Authorization vulnerability in SecuPress SecuPress Free secupress.This issue affects SecuPress Free: from n/a through <= 2.2.5.3.	N/A	More Details
CVE-2024-34438	Missing Authorization vulnerability in Anssi Laitila Shared Files shared-files.This issue affects Shared Files: from n/a through <= 1.7.19.	N/A	More Details
CVE-2026-21627	The vulnerability was rooted in how the Tassos Framework plugin handled specific AJAX requests through Joomla’s com_ajax entry point. Under certain conditions, internal framework functionality could be invoked without proper restriction.	N/A	More Details
CVE-2025-14055	An integer underflow vulnerability in Silicon Labs Secure NCP host implementation allows a buffer overread via a specially crafted packet.	N/A	More Details
CVE-2026-27317	Rejected reason: Not used	N/A	More Details
CVE-2026-21620	Relative Path Traversal, Improper Isolation or Compartmentalization vulnerability in erlang otp erlang/otp (tftp_file modules), erlang otp inets (tftp_file modules), erlang otp tftp (tftp_file modules) allows Relative Path Traversal. This vulnerability is associated with program files lib/tftp/src/tftp_file.erl, src/tftp_file.erl. This issue affects otp: from 17.0, from 07b8f441ca711f9812fad9e9115bab3c3aa92f79; otp: from 5.10 before 7.0; otp: from 1.0.	N/A	More Details
CVE-2026-26050	The installer for ジョブログ集計/分析ソフトウェア RICOHジョブログ集計ツール versions prior to Ver.1.3.7 contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with administrative privileges.	N/A	More Details
CVE-2026-26370	WordPress Plugin "Survey Maker" versions 5.1.7.7 and prior contain a cross-site scripting vulnerability. If this vulnerability is exploited, an arbitrary script may be executed in the user's web browser.	N/A	More Details
CVE-2026-27325	Rejected reason: Not used	N/A	More Details
CVE-2026-27324	Rejected reason: Not used	N/A	More Details
CVE-2026-27323	Rejected reason: Not used	N/A	More Details
CVE-2026-27322	Rejected reason: Not used	N/A	More Details
CVE-2026-27321	Rejected reason: Not used	N/A	More Details
CVE-2026-27320	Rejected reason: Not used	N/A	More Details
CVE-2026-27319	Rejected reason: Not used	N/A	More Details
CVE-2026-27318	Rejected reason: Not used	N/A	More Details
CVE-2026-2731	Path traversal and content injection in JobRunnerBackground.aspx in DynamicWeb 8 (all) and 9 (<9.19.7 and <9.20.3) allows unauthenticated attackers to execute code via simple web requests	N/A	More Details
CVE-2025-	OGP-Website installs prior git commit 52f865a4fba763594453068acf8fa9e3fc38d663 are affected by a type juggling flaw which	N/A	More

15586	if exploited can result in authentication bypass without knowledge of the victim account's password.		Details
CVE-2026-25984	Rejected reason: This CVE was assigned in error.	N/A	More Details
CVE-2025-71237	In the Linux kernel, the following vulnerability has been resolved: nilfs2: Fix potential block overflow that cause system hang When a user executes the FITRIM command, an underflow can occur when calculating nblocks if end_block is too small. Since nblocks is of type sector_t, which is u64, a negative nblocks value will become a very large positive integer. This ultimately leads to the block layer function __blkdev_issue_discard() taking an excessively long time to process the bio chain, and the ns_segctor_sem lock remains held for a long period. This prevents other tasks from acquiring the ns_segctor_sem lock, resulting in the hang reported by syzbot in [1]. If the ending block is too small, typically if it is smaller than 4KiB range, depending on the usage of the segment 0, it may be possible to attempt a discard request beyond the device size causing the hang. Exiting successfully and assign the discarded size (0 in this case) to range->len. Although the start and len values in the user input range are too small, a conservative strategy is adopted here to safely ignore them, which is equivalent to a no-op; it will not perform any trimming and will not throw an error. [1] task:segctord state:D stack:28968 pid:6093 tgid:6093 ppid:2 task_flags:0x200040 flags:0x00080000 Call Trace: rwbase_write_lock+0x3dd/0x750 kernel/locking/rwbase_rt.c:272 nilfs_transaction_lock+0x253/0x4c0 fs/nilfs2/segment.c:357 nilfs_segctor_thread_construct fs/nilfs2/segment.c:2569 [inline] nilfs_segctor_thread+0x6ec/0xe00 fs/nilfs2/segment.c:2684 [ryusuke: corrected part of the commit message about the consequences]	N/A	More Details
CVE-2026-23218	In the Linux kernel, the following vulnerability has been resolved: gpio: loongson-64bit: Fix incorrect NULL check after devm_kcalloc() Fix incorrect NULL check in loongson_gpio_init_irqchip(). The function checks chip->parent instead of chip->irq.parents.	N/A	More Details
CVE-2026-23219	In the Linux kernel, the following vulnerability has been resolved: mm/slab: Add alloc_tagging_slab_free_hook for memcg_alloc_abort_single When CONFIG_MEM_ALLOC_PROFILING_DEBUG is enabled, the following warning may be noticed: [3959.023862] ------------[cut here]------------ [3959.023891] alloc_tag was not cleared (got tag for lib/xarray.c:378) [3959.023947] WARNING: ./include/linux/alloc_tag.h:155 at alloc_tag_add+0x128/0x178, CPU#6: mkfs.ntfs/113998 [3959.023978] Modules linked in: dns_resolver tun brd overlay exfat btrfs blake2b libblake2b xor xor_neon raid6_pq loop sctp ip6_udp_tunnel udp_tunnel ext4 crc16 mbcache jbd2 rfkill sunrpc vfat fat sg fuse nfnetlink sr_mod virtio_gpu cdrom drm_client_lib virtio_dma_buf drm_shmem_helper drm_kms_helper ghash_ce drm sm4 backlight virtio_net net_failover virtio_scsi failover virtio_console virtio_blk virtio_mmio dm_mirror dm_region_hash dm_log dm_multipath dm_mod i2c_dev aes_neon_bs aes_ce_blk [last unloaded: hwpoison_inject] [3959.024170] CPU: 6 UID: 0 PID: 113998 Comm: mkfs.ntfs Kdump: loaded Tainted: G W 6.19.0-rc7+ #7 PREEMPT(voluntary) [3959.024182] Tainted: [W]=WARN [3959.024186] Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 [3959.024192] pstate: 604000c5 (nZCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3959.024199] pc : alloc_tag_add+0x128/0x178 [3959.024207] lr : alloc_tag_add+0x128/0x178 [3959.024214] sp : ffff80008b696d60 [3959.024219] x29: ffff80008b696d60 x28: 0000000000000000 x27: 0000000000000240 [3959.024232] x26: 0000000000000000 x25: 0000000000000240 x24: ffff800085d17860 [3959.024245] x23: 0000000000402800 x22: ffff0000c0012dc0 x21: 00000000000002d0 [3959.024257] x20: ffff0000e6ef3318 x19: ffff800085ae0410 x18: 0000000000000000 [3959.024269] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [3959.024281] x14: 0000000000000000 x13: 0000000000000001 x12: ffff600064101293 [3959.024292] x11: 1fffe00064101292 x10: ffff600064101292 x9 : dfff800000000000 [3959.024305] x8 : 00009fff9befed6e x7 : ffff000320809493 x6 : 0000000000000001 [3959.024316] x5 : ffff000320809490 x4 : ffff600064101293 x3 : ffff800080691838 [3959.024328] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000d5bcd640 [3959.024340] Call trace: [3959.024346] alloc_tag_add+0x128/0x178 (P) [3959.024355] __alloc_tagging_slab_alloc_hook+0x11c/0x1a8 [3959.024362] kmem_cache_alloc_lru_noprof+0x1b8/0x5e8 [3959.024369] xas_alloc+0x304/0x4f0 [3959.024381] xas_create+0x1e0/0x4a0 [3959.024388] xas_store+0x68/0xda8 [3959.024395] __filemap_add_folio+0x5b0/0xbd8 [3959.024409] filemap_add_folio+0x16c/0x7e0 [3959.024416] __filemap_get_folio_mpol+0x2dc/0x9e8 [3959.024424] iomap_get_folio+0xfc/0x180 [3959.024435] __iomap_get_folio+0x2f8/0x4b8 [3959.024441] iomap_write_begin+0x198/0xc18 [3959.024448] iomap_write_iter+0x2ec/0x8f8 [3959.024454] iomap_file_buffered_write+0x19c/0x290 [3959.024461] blkdev_write_iter+0x38c/0x978 [3959.024470] vfs_write+0x4d4/0x928 [3959.024482] ksys_write+0xfc/0x1f8 [3959.024489] __arm64_sys_write+0x74/0xb0 [3959.024496] invoke_syscall+0xd4/0x258 [3959.024507] el0_svc_common.constprop.0+0xb4/0x240 [3959.024514] do_el0_svc+0x48/0x68 [3959.024520] el0_svc+0x40/0xf8 [3959.024526] el0t_64_sync_handler+0xa0/0xe8 [3959.024533] el0t_64_sync+0x1ac/0x1b0 [3959.024540] ---[end trace 0000000000000000]--- When __memcg_slab_post_alloc_hook() fails, there are two different free paths depending on whether size == 1 or size != 1. In the kmem_cache_free_bulk() path, we do call alloc_tagging_slab_free_hook(). However, in memcg_alloc_abort_single() we don't, the above warning will be triggered on the next allocation. Therefore, add alloc_tagging_slab_free_hook() to the memcg_alloc_abort_single() path.	N/A	More Details
CVE-2025-15579	Deserialization of Untrusted Data vulnerability in OpenText™ Directory Services allows Object Injection. The vulnerability could lead to remote code execution, denial of service, or privilege escalation. This issue affects Directory Services: from 10.5 through 26.1.	N/A	More Details
CVE-2025-71229	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: Fix alignment fault in rtw_core_enable_beacon() rtw_core_enable_beacon() reads 4 bytes from an address that is not a multiple of 4. This results in a crash on some systems. Do 1 byte reads/writes instead. Unable to handle kernel paging request at virtual address ffff8000827e0522 Mem abort info: ESR = 0x0000000096000021 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x21: alignment fault Data abort info: ISV = 0, ISS = 0x00000021, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 swapper pgtable: 4k pages, 48-bit VAs, pgdp=0000000005492000 [ffff8000827e0522] pgd=0000000000000000, p4d=10000001021d9403, pud=10000001021da403, pmd=100000011061c403, pte=00780000f3200f13 Internal error: Oops: 0000000096000021 [#1] SMP Modules linked in: [...] rtw88_8822ce rtw88_8822c rtw88_pci rtw88_core [...] CPU: 0 UID: 0 PID: 73 Comm: kworker/u32:2 Tainted: G W 6.17.9 #1-NixOS VOLUNTARY Tainted: [W]=WARN Hardware name: FriendlyElec NanoPC-T6 LTS (DT) Workqueue: phy0 rtw_c2h_work [rtw88_core] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : rtw_pci_read32+0x18/0x40 [rtw88_pci] lr : rtw_core_enable_beacon+0xe0/0x148 [rtw88_core] sp : ffff800080cc3ca0 x29: ffff800080cc3ca0 x28: ffff0001031fc240 x27: ffff000102100828 x26: ffffd2cb7c9b4088 x25: ffff0001031fc2c0 x24: ffff000112fdef00 x23: ffff000112fdef18 x22: ffff000111c29970 x21: 0000000000000001 x20: 0000000000000001 x19: ffff000111c22040 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000	N/A	More Details

	x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffd2cb6507c090 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000007f10 x1 : 0000000000000522 x0 : ffff8000827e0522 Call trace: rtw_pci_read32+0x18/0x40 [rtw88_pci] (P) rtw_hw_scan_chan_switch+0x124/0x1a8 [rtw88_core] rtw_fw_c2h_cmd_handle+0x254/0x290 [rtw88_core] rtw_c2h_work+0x50/0x98 [rtw88_core] process_one_work+0x178/0x3f8 worker_thread+0x208/0x418 kthread+0x120/0x220 ret_from_fork+0x10/0x20 Code: d28fe202 8b020000 f9524400 8b214000 (b9400000) ---[end trace 0000000000000000]---		
CVE-2025-71230	In the Linux kernel, the following vulnerability has been resolved: hfs: ensure sb->s_fs_info is always cleaned up When hfs was converted to the new mount api a bug was introduced by changing the allocation pattern of sb->s_fs_info. If setup_bdev_super() fails after a new superblock has been allocated by sget_fc(), but before hfs_fill_super() takes ownership of the filesystem-specific s_fs_info data it was leaked. Fix this by freeing sb->s_fs_info in hfs_kill_super().	N/A	More Details
CVE-2025-71231	In the Linux kernel, the following vulnerability has been resolved: crypto: iaa - Fix out-of-bounds index in find_empty_iaa_compression_mode The local variable 'i' is initialized with -EINVAL, but the for loop immediately overwrites it and -EINVAL is never returned. If no empty compression mode can be found, the function would return the out-of-bounds index IAA_COMP_MODES_MAX, which would cause an invalid array access in add_iaa_compression_mode(). Fix both issues by returning either a valid index or -EINVAL.	N/A	More Details
CVE-2025-71232	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Free sp in error path to fix system crash System crash seen during load/unload test in a loop, [61110.449331] qla2xxx [0000:27:00.0]-0042:0: Disabled MSI-X. [61110.467494] == [61110.467498] BUG qla2xxx_srbs (Tainted: G OE -------- ---): Objects remaining in qla2xxx_srbs on __kmem_cache_shutdown() [61110.467501] ---------- [61110.467502] Slab 0x000000000ffc8162 objects=51 used=1 fp=0x00000000e25d3d85 flags=0x57ffffc0010200(slab|head|node=1|zone=2|lastcpupid=0x1fffff) [61110.467509] CPU: 53 PID: 455206 Comm: rmmod Kdump: loaded Tainted: G OE -------- --- 5.14.0-284.11.1.el9_2.x86_64 #1 [61110.467513] Hardware name: HPE ProLiant DL385 Gen10 Plus v2/ProLiant DL385 Gen10 Plus v2, BIOS A42 08/17/2023 [61110.467515] Call Trace: [61110.467516] <TASK> [61110.467519] dump_stack_lvl+0x34/0x48 [61110.467526] slab_err.cold+0x53/0x67 [61110.467534] __kmem_cache_shutdown+0x16e/0x320 [61110.467540] kmem_cache_destroy+0x51/0x160 [61110.467544] qla2x00_module_exit+0x93/0x99 [qla2xxx] [61110.467607] ? __do_sys_delete_module.constprop.0+0x178/0x280 [61110.467613] ? syscall_trace_enter.constprop.0+0x145/0x1d0 [61110.467616] ? do_syscall_64+0x5c/0x90 [61110.467619] ? exc_page_fault+0x62/0x150 [61110.467622] ? entry_SYSCALL_64_after_hwframe+0x63/0xcd [61110.467626] </TASK> [61110.467627] Disabling lock debugging due to kernel taint [61110.467635] Object 0x0000000026f7e6e6 @offset=16000 [61110.467639] ------------[cut here]------------ [61110.467639] kmem_cache_destroy qla2xxx_srbs: Slab cache still has objects when called from qla2x00_module_exit+0x93/0x99 [qla2xxx] [61110.467659] WARNING: CPU: 53 PID: 455206 at mm/slab_common.c:520 kmem_cache_destroy+0x14d/0x160 [61110.467718] CPU: 53 PID: 455206 Comm: rmmod Kdump: loaded Tainted: G B OE -------- --- 5.14.0-284.11.1.el9_2.x86_64 #1 [61110.467720] Hardware name: HPE ProLiant DL385 Gen10 Plus v2/ProLiant DL385 Gen10 Plus v2, BIOS A42 08/17/2023 [61110.467721] RIP: 0010:kmem_cache_destroy+0x14d/0x160 [61110.467724] Code: 99 7d 07 00 48 89 ef e8 e1 6a 07 00 eb b3 48 8b 55 60 48 8b 4c 24 20 48 c7 c6 70 fc 66 90 48 c7 c7 f8 ef a1 90 e8 e1 ed 7c 00 <0f> 0b eb 93 c3 cc cc cc cc 66 2e 0f 1f 84 00 00 00 00 00 55 48 89 [61110.467725] RSP: 0018:ffffa304e489fe80 EFLAGS: 00010282 [61110.467727] RAX: 0000000000000000 RBX: ffffffffc0d9a860 RCX: 0000000000000027 [61110.467729] RDX: ffff8fd5ff9598a8 RSI: 0000000000000001 RDI: ffff8fd5ff9598a0 [61110.467730] RBP: ffff8fb6aaf78700 R08: 0000000000000000 R09: 0000000100d863b7 [61110.467731] R10: ffffa304e489fd20 R11: ffffffff913bef48 R12: 0000000040002000 [61110.467731] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [61110.467733] FS: 00007f64c89fb740(0000) GS:ffff8fd5ff940000(0000) knlGS:0000000000000000 [61110.467734] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [61110.467735] CR2: 00007f0f02bfe000 CR3: 00000020ad6dc005 CR4: 0000000000770ee0 [61110.467736] PKRU: 55555554 [61110.467737] Call Trace: [61110.467738] <TASK> [61110.467739] qla2x00_module_exit+0x93/0x99 [qla2xxx] [61110.467755] ? __do_sys_delete_module.constprop.0+0x178/0x280 Free sp in the error path to fix the crash.	N/A	More Details
CVE-2025-71233	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: Avoid creating sub-groups asynchronously The asynchronous creation of sub-groups by a delayed work could lead to a NULL pointer dereference when the driver directory is removed before the work completes. The crash can be easily reproduced with the following commands: # cd /sys/kernel/config/pci_ep/functions/pci_epf_test # for i in {1..20}; do mkdir test && rmdir test; done BUG: kernel NULL pointer dereference, address: 0000000000000088 ... Call Trace: configfs_register_group+0x3d/0x190 pci_epf_cfs_work+0x41/0x110 process_one_work+0x18f/0x350 worker_thread+0x25a/0x3a0 Fix this issue by using configfs_add_default_group() API which does not have the deadlock problem as configfs_register_group() and does not require the delayed work handler. [mani: slightly reworded the description and added stable list]	N/A	More Details
CVE-2025-71234	In the Linux kernel, the following vulnerability has been resolved: wifi: rtl8xxxu: fix slab-out-of-bounds in rtl8xxxu_sta_add The driver does not set hw->sta_data_size, which causes mac80211 to allocate insufficient space for driver private station data in __sta_info_alloc(). When rtl8xxxu_sta_add() accesses members of struct rtl8xxxu_sta_info through sta->drv_priv, this results in a slab-out-of-bounds write. KASAN report on RISC-V (VisionFive 2) with RTL8192EU adapter: BUG: KASAN: slab-out-of-bounds in rtl8xxxu_sta_add+0x31c/0x346 Write of size 8 at addr ffffffd6d3e9ae88 by task kworker/u16:0/12 Set hw->sta_data_size to sizeof(struct rtl8xxxu_sta_info) during probe, similar to how hw->vif_data_size is configured. This ensures mac80211 allocates sufficient space for the driver's per-station private data. Tested on StarFive VisionFive 2 v1.2A board.	N/A	More Details
CVE-2025-71235	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Delay module unload while fabric scan in progress System crash seen during load/unload test in a loop. [105954.384919] RBP: ffff914589838dc0 R08: 0000000000000000 R09: 0000000000000086 [105954.384920] R10: 000000000000000f R11: ffffa31240904be5 R12: ffff914605f868e0 [105954.384921] R13: ffff914605f86910 R14: 0000000000008010 R15: 00000000ddb7c000 [105954.384923] FS: 0000000000000000(0000) GS:ffff9163fec40000(0000) knlGS:0000000000000000 [105954.384925] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [105954.384926] CR2: 000055d31ce1d6a0 CR3: 0000000119f5e001 CR4: 0000000000770ee0 [105954.384928] PKRU: 55555554 [105954.384929] Call Trace: [105954.384931] <IRQ> [105954.384934] qla24xx_sp_unmap+0x1f3/0x2a0 [qla2xxx] [105954.384962] ? qla_async_scan_sp_done+0x114/0x1f0 [qla2xxx] [105954.384980] ? qla24xx_els_ct_entry+0x4de/0x760 [qla2xxx] [105954.384999] ? __wake_up_common+0x80/0x190 [105954.385004] ? qla24xx_process_response_queue+0xc2/0xaa0 [qla2xxx] [105954.385023] ? qla24xx_msix_rsp_q+0x44/0xb0 [qla2xxx] [105954.385040] ? __handle_irq_event_percpu+0x3d/0x190 [105954.385044] ? handle_irq_event+0x58/0xb0 [105954.385046] ? handle_edge_irq+0x93/0x240 [105954.385050] ? __common_interrupt+0x41/0xa0 [105954.385055] ? common_interrupt+0x3e/0xa0 [105954.385060] ?	N/A	More Details

	asm_common_interrupt+0x22/0x40 The root cause of this was that there was a free (dma_free_attrs) in the interrupt context. There was a device discovery/fabric scan in progress. A module unload was issued which set the UNLOADING flag. As part of the discovery, after receiving an interrupt a work queue was scheduled (which involved a work to be queued). Since the UNLOADING flag is set, the work item was not allocated and the mapped memory had to be freed. The free occurred in interrupt context leading to system crash. Delay the driver unload until the fabric scan is complete to avoid the crash.		
CVE-2025-71236	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Validate sp before freeing associated memory System crash with the following signature [154563.214890] nvme nvme2: NVME-FC{1}: controller connect complete [154564.169363] qla2xxx [0000:b0:00.1]-3002:2: nvme: Sched: Set ZIO exchange threshold to 3. [154564.169405] qla2xxx [0000:b0:00.1]-ffffff:2: SET ZIO Activity exchange threshold to 5. [154565.539974] qla2xxx [0000:b0:00.1]-5013:2: RSCN database changed – 0078 0080 0000. [154565.545744] qla2xxx [0000:b0:00.1]-5013:2: RSCN database changed – 0078 00a0 0000. [154565.545857] qla2xxx [0000:b0:00.1]-11a2:2: FEC=enabled (data rate). [154565.552760] qla2xxx [0000:b0:00.1]-11a2:2: FEC=enabled (data rate). [154565.553079] BUG: kernel NULL pointer dereference, address: 00000000000000f8 [154565.553080] #PF: supervisor read access in kernel mode [154565.553082] #PF: error_code(0x0000) - not-present page [154565.553084] PGD 80000010488ab067 P4D 80000010488ab067 PUD 104978a067 PMD 0 [154565.553089] Oops: 0000 1 PREEMPT SMP PTI [154565.553092] CPU: 10 PID: 858 Comm: qla2xxx_2_dpc Kdump: loaded Tainted: G OE ------- --- 5.14.0-503.11.1.el9_5.x86_64 #1 [154565.553096] Hardware name: HPE Synergy 660 Gen10/Synergy 660 Gen10 Compute Module, BIOS I43 09/30/2024 [154565.553097] RIP: 0010:qla_fab_async_scan.part.0+0x40b/0x870 [qla2xxx] [154565.553141] Code: 00 00 e8 58 a3 ec d4 49 89 e9 ba 12 20 00 00 4c 89 e6 49 c7 c0 00 ee a8 c0 48 c7 c1 66 c0 a9 c0 bf 00 80 00 10 e8 15 69 00 00 <4c> 8b 8d f8 00 00 00 4d 85 c9 74 35 49 8b 84 24 00 19 00 00 48 8b [154565.553143] RSP: 0018:ffffb4dbc8aebdd0 EFLAGS: 00010286 [154565.553145] RAX: 0000000000000000 RBX: ffff8ec2cf0908d0 RCX: 0000000000000002 [154565.553147] RDX: 0000000000000000 RSI: ffffffffc0a9c896 RDI: ffffb4dbc8aebd47 [154565.553148] RBP: 0000000000000000 R08: ffffb4dbc8aebd45 R09: 0000000000ffff0a [154565.553150] R10: 0000000000000000 R11: 000000000000000f R12: ffff8ec2cf0908d0 [154565.553151] R13: ffff8ec2cf090900 R14: 0000000000000102 R15: ffff8ec2cf084000 [154565.553152] FS: 0000000000000000(0000) GS:ffff8ed27f800000(0000) knlGS:0000000000000000 [154565.553154] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [154565.553155] CR2: 00000000000000f8 CR3: 000000113ae0a005 CR4: 00000000007706f0 [154565.553157] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [154565.553158] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [154565.553159] PKRU: 55555554 [154565.553160] Call Trace: [154565.553162] <TASK> [154565.553165] ? show_trace_log_lvl+0x1c4/0x2df [154565.553172] ? show_trace_log_lvl+0x1c4/0x2df [154565.553177] ? qla_fab_async_scan.part.0+0x40b/0x870 [qla2xxx] [154565.553215] ? __die_body.cold+0x8/0xd [154565.553218] ? page_fault_oops+0x134/0x170 [154565.553223] ? snprintf+0x49/0x70 [154565.553229] ? exc_page_fault+0x62/0x150 [154565.553238] ? asm_exc_page_fault+0x22/0x30 Check for sp being non NULL before freeing any associated memory	N/A	More Details
CVE-2026-23220	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix infinite loop caused by next_smb2_rcv_hdr_off reset in error paths The problem occurs when a signed request fails smb2 signature verification check. In __process_request(), if check_sign_req() returns an error, set_smb2_rsp_status(work, STATUS_ACCESS_DENIED) is called. set_smb2_rsp_status() set work->next_smb2_rcv_hdr_off as zero. By resetting next_smb2_rcv_hdr_off to zero, the pointer to the next command in the chain is lost. Consequently, is_chained_smb2_message() continues to point to the same request header instead of advancing. If the header's NextCommand field is non-zero, the function returns true, causing __handle_ksmbd_work() to repeatedly process the same failed request in an infinite loop. This results in the kernel log being flooded with "bad smb2 signature" messages and high CPU usage. This patch fixes the issue by changing the return value from SERVER_HANDLER_CONTINUE to SERVER_HANDLER_ABORT. This ensures that the processing loop terminates immediately rather than attempting to continue from an invalidated offset.	N/A	More Details
CVE-2026-23216	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Fix use-after-free in iscsit_dec_conn_usage_count() In iscsit_dec_conn_usage_count(), the function calls complete() while holding the conn->conn_usage_lock. As soon as complete() is invoked, the waiter (such as iscsit_close_connection()) may wake up and proceed to free the iscsit_conn structure. If the waiter frees the memory before the current thread reaches spin_unlock_bh(), it results in a KASAN slab-use-after-free as the function attempts to release a lock within the already-freed connection structure. Fix this by releasing the spinlock before calling complete().	N/A	More Details
CVE-2026-23221	In the Linux kernel, the following vulnerability has been resolved: bus: fsl-mc: fix use-after-free in driver_override_show() The driver_override_show() function reads the driver_override string without holding the device_lock. However, driver_override_store() uses driver_set_override(), which modifies and frees the string while holding the device_lock. This can result in a concurrent use-after-free if the string is freed by the store function while being read by the show function. Fix this by holding the device_lock around the read operation.	N/A	More Details
CVE-2026-23222	In the Linux kernel, the following vulnerability has been resolved: crypto: omap - Allocate OMAP_CRYPTO_FORCE_COPY scatterlists correctly The existing allocation of scatterlists in omap_crypto_copy_sg_lists() was allocating an array of scatterlist pointers, not scatterlist objects, resulting in a 4x too small allocation. Use sizeof(*new_sg) to get the correct object size.	N/A	More Details
CVE-2026-23223	In the Linux kernel, the following vulnerability has been resolved: xfs: fix UAF in xchk_btree_check_block_owner We cannot dereference bs->cur when trying to determine if bs->cur aliases bs->sc->sa.{bno,rmap}_cur after the latter has been freed. Fix this by sampling before type before any freeing could happen. The correct temporal ordering was broken when we removed xfs_btnum_t.	N/A	More Details
CVE-2026-23224	In the Linux kernel, the following vulnerability has been resolved: erofs: fix UAF issue for file-backed mounts w/ directio option [9.269940][T3222] Call trace: [9.269948][T3222] ext4_file_read_iter+0xac/0x108 [9.269979][T3222] vfs_iocb_iter_read+0xac/0x198 [9.269993][T3222] erofs_fileio_rq_submit+0x12c/0x180 [9.270008][T3222] erofs_fileio_submit_bio+0x14/0x24 [9.270030][T3222] z_erofs_runqueue+0x834/0x8ac [9.270054][T3222] z_erofs_read_folio+0x120/0x220 [9.270083][T3222] filemap_read_folio+0x60/0x120 [9.270102][T3222] filemap_fault+0xcac/0x1060 [9.270119][T3222] do_pte_missing+0x2d8/0x1554 [9.270131][T3222] handle_mm_fault+0x5ec/0x70c [9.270142][T3222] do_page_fault+0x178/0x88c [9.270167][T3222] do_translation_fault+0x38/0x54 [9.270183][T3222] do_mem_abort+0x54/0xac [9.270208][T3222] el0_da+0x44/0x7c [9.270227][T3222] el0t_64_sync_handler+0x5c/0xf4 [9.270253][T3222] el0t_64_sync+0x1bc/0x1c0 EROFS may encounter above panic when enabling file-backed mount w/ directio mount option, the root cause is it may suffer UAF in below race condition: - z_erofs_read_folio wq s_dio_done_wq - z_erofs_runqueue - erofs_fileio_submit_bio - erofs_fileio_rq_submit - vfs_iocb_iter_read - ext4_file_read_iter - ext4_dio_read_iter - iomap_dio_rw : bio was submitted and return -EIOCBQUEUED - dio_aio_complete_work - dio_complete - dio->iocb->ki_complete (erofs_fileio_ki_complete()) - kfree(rq) : it frees iocb, iocb.ki_filp	N/A	More Details

	can be UAF in file_accessed(). - file_accessed : access NULL file point Introduce a reference count in struct erofs_fileio_rq, and initialize it as two, both erofs_fileio_ki_complete() and erofs_fileio_rq_submit() will decrease reference count, the last one decreasing the reference count to zero will free rq.		
CVE-2026-23225	In the Linux kernel, the following vulnerability has been resolved: sched/mmcid: Don't assume CID is CPU owned on mode switch Shinichiro reported a KASAN UAF, which is actually an out of bounds access in the MMCID management code. CPU0 CPU1 T1 runs in userspace T0: fork(T4) -> Switch to per CPU CID mode fixup() set MM_CID_TRANSIT on T1/CPU1 T4 exit() T3 exit() T2 exit() T1 exit() switch to per task mode ---> Out of bounds access. As T1 has not scheduled after T0 set the TRANSIT bit, it exits with the TRANSIT bit set. sched_mm_cid_remove_user() clears the TRANSIT bit in the task and drops the CID, but it does not touch the per CPU storage. That's functionally correct because a CID is only owned by the CPU when the ONCPU bit is set, which is mutually exclusive with the TRANSIT flag. Now sched_mm_cid_exit() assumes that the CID is CPU owned because the prior mode was per CPU. It invokes mm_drop_cid_on_cpu() which clears the not set ONCPU bit and then invokes clear_bit() with an insanely large bit number because TRANSIT is set (bit 29). Prevent that by actually validating that the CID is CPU owned in mm_drop_cid_on_cpu().	N/A	More Details
CVE-2026-23226	In the Linux kernel, the following vulnerability has been resolved: ksmbd: add chann_lock to protect ksmbd_chann_list xarray ksmbd_chann_list xarray lacks synchronization, allowing use-after-free in multi-channel sessions (between lookup_chann_list() and ksmbd_chann_del). Adds rw_semaphore chann_lock to struct ksmbd_session and protects all xa_load/xa_store/xa_erase accesses.	N/A	More Details
CVE-2026-23227	In the Linux kernel, the following vulnerability has been resolved: drm/exynos: vidi: use ctx->lock to protect struct vidi_context member variables related to memory alloc/free Exynos Virtual Display driver performs memory alloc/free operations without lock protection, which easily causes concurrency problem. For example, use-after-free can occur in race scenario like this: ``` CPU0 CPU1 CPU2 ---- ---- ---- vidi_connection_ioctl() if (vidi->connection) // true drm_edid = drm_edid_alloc(); // alloc drm_edid ... ctx->raw_edid = drm_edid; ... drm_mode_getconnector() drm_helper_probe_single_connector_modes() vidi_get_modes() if (ctx->raw_edid) // true drm_edid_dup(ctx->raw_edid); if (!drm_edid) // false ... vidi_connection_ioctl() if (vidi->connection) // false drm_edid_free(ctx->raw_edid); // free drm_edid ... drm_edid_alloc(drm_edid->edid) kmemdup(edid); // UAF!! ... ``` To prevent these vulns, at least in vidi_context, member variables related to memory alloc/free should be protected with ctx->lock.	N/A	More Details
CVE-2026-23228	In the Linux kernel, the following vulnerability has been resolved: smb: server: fix leak of active_num_conn in ksmbd_tcp_new_connection() On kthread_run() failure in ksmbd_tcp_new_connection(), the transport is freed via free_transport(), which does not decrement active_num_conn, leaking this counter. Replace free_transport() with ksmbd_tcp_disconnect().	N/A	More Details
CVE-2026-23229	In the Linux kernel, the following vulnerability has been resolved: crypto: virtio - Add spinlock protection with virtqueue notification When VM boots with one virtio-crypto PCI device and builtin backend, run openssl benchmark command with multiple processes, such as openssl speed -evp aes-128-cbc -engine afalg -seconds 10 -multi 32 openssl processes will hangup and there is error reported like this: virtio_crypto virtio0: dataq.0:id 3 is not a head! It seems that the data virtqueue need protection when it is handled for virtio done notification. If the spinlock protection is added in virtcrypto_done_task(), openssl benchmark with multiple processes works well.	N/A	More Details
CVE-2026-23230	In the Linux kernel, the following vulnerability has been resolved: smb: client: split cached_fid bitfields to avoid shared-byte RMW races is_open, has_lease and on_list are stored in the same bitfield byte in struct cached_fid but are updated in different code paths that may run concurrently. Bitfield assignments generate byte read–modify–write operations (e.g. `orb $mask, addr` on x86_64), so updating one flag can restore stale values of the others. A possible interleaving is: CPU1: load old byte (has_lease=1, on_list=1) CPU2: clear both flags (store 0) CPU1: RMW store (old | IS_OPEN) -> reintroduces cleared bits To avoid this class of races, convert these flags to separate bool fields.	N/A	More Details
CVE-2025-13602	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-23217	In the Linux kernel, the following vulnerability has been resolved: riscv: trace: fix snapshot deadlock with sbi ecall If sbi_ecall.c's functions are traceable, echo "__sbi_ecall:snapshot" > /sys/kernel/tracing/set_ftrace_filter may get the kernel into a deadlock. (Functions in sbi_ecall.c are excluded from tracing if CONFIG_RISCV_ALTERNATIVE_EARLY is set.) __sbi_ecall triggers a snapshot of the ringbuffer. The snapshot code raises an IPI interrupt, which results in another call to __sbi_ecall and another snapshot... All it takes to get into this endless loop is one initial __sbi_ecall. On RISC-V systems without SSTC extension, the clock events in timer-riscv.c issue periodic sbi ecalls, making the problem easy to trigger. Always exclude the sbi_ecall.c functions from tracing to fix the potential deadlock. sbi ecalls can easiliy be logged via trace events, excluding ecall functions from function tracing is not a big limitation.	N/A	More Details
CVE-2026-23215	In the Linux kernel, the following vulnerability has been resolved: x86/vmware: Fix hypercall clobbers Fedora QA reported the following panic: BUG: unable to handle page fault for address: 0000000040003e54 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS edk2-20251119-3.fc43 11/19/2025 RIP: 0010:vmware_hypercall4.constprop.0+0x52/0x90 .. Call Trace: vmmouse_report_events+0x13e/0x1b0 psmouse_handle_byte+0x15/0x60 ps2_interrupt+0x8a/0xd0 ... because the QEMU VMware mouse emulation is buggy, and clears the top 32 bits of %rdi that the kernel kept a pointer in. The QEMU vmmouse driver saves and restores the register state in a "uint32_t data[6];" and as a result restores the state with the high bits all cleared. RDI originally contained the value of a valid kernel stack address (0xff5eeb3240003e54). After the vmware hypercall it now contains 0x40003e54, and we get a page fault as a result when it is dereferenced. The proper fix would be in QEMU, but this works around the issue in the kernel to keep old setups working, when old kernels had not happened to keep any state in %rdi over the hypercall. In theory this same issue exists for all the hypercalls in the vmmouse driver; in practice it has only been seen with vmware_hypercall3() and vmware_hypercall4(). For now, just mark RDI/RSI as clobbered for those two calls. This should have a minimal effect on code generation overall as it should be rare for the compiler to want to make RDI/RSI live across hypercalls.	N/A	More Details
CVE-2025-13965	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-12500. Reason: This candidate is a reservation duplicate of CVE-2025-12500. Notes: All CVE users should reference CVE-2025-12500 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-	An issue pertaining to CWE-295: Improper Certificate Validation was discovered in YMFE yapi v1.12.0. The application disables		More

2025-70058	TLS/SSL certificate validation by setting 'rejectUnauthorized': false in the HTTPS agent configuration for Axios requests	N/A	Details
CVE-2025-69248	free5GC is an open-source project for 5th generation (5G) mobile core networks. Versions up to and including 1.4.1 of free5GC's AMF service have a Buffer Overflow vulnerability leading to Denial of Service. Remote unauthenticated attackers can crash the AMF service by sending a specially crafted NAS Registration Request with a malformed 5GS Mobile Identity, causing complete denial of service for the 5G core network. All deployments of free5GC using the AMF component may be affected. Pull request 43 of the free5gc/nas repo contains a fix. No direct workaround is available at the application level. Applying the official patch is recommended.	N/A	More Details
CVE-2025-69247	free5GC go-upf is the User Plane Function (UPF) implementation for 5G networks that is part of the free5GC project. Versions prior to 1.2.8 have a Heap-based Buffer Overflow (CWE-122) vulnerability leading to Denial of Service. Remote attackers can crash the UPF network element by sending a specially crafted PFCP Session Modification Request with an invalid SDF Filter length field. This causes a heap buffer overflow, resulting in complete service disruption for all connected UEs and potential cascading failures affecting the SMF. All deployments of free5GC using the UPF component may be affected. Version 1.2.8 of go-upf contains a fix.	N/A	More Details
CVE-2025-69232	free5GC is an open-source project for 5th generation (5G) mobile core networks. free5GC go-upf versions up to and including 1.2.6, corresponding to free5gc smf up to and including 1.4.0, have an Improper Input Validation and Protocol Compliance vulnerability leading to Denial of Service. Remote attackers can disrupt core network functionality by sending a malformed PFCP Association Setup Request. The UPF incorrectly accepts it, entering an inconsistent state that causes subsequent legitimate requests to trigger SMF reconnection loops and service degradation. All deployments of free5GC using the UPF and SMF components may be affected. As of time of publication, a fix is in development but not yet available. No direct workaround is available at the application level. Applying the official patch, once released, is recommended.	N/A	More Details
CVE-2025-69208	free5GC UDR is the user data repository (UDR) for free5GC, an an open-source project for 5th generation (5G) mobile core networks. Versions prior to 1.4.1 contain an Improper Error Handling vulnerability with Information Exposure. All deployments of free5GC using the Nnef_PfdManagement service may be affected. The NEF component reliably leaks internal parsing errors (e.g., invalid character 'n' after top-level value) to remote clients. This can aid attackers in fingerprinting server software and logic flows. Version 1.4.1 fixes the issue. There is no direct workaround at the application level. The recommended mitigation is to apply the provided patch.	N/A	More Details
CVE-2026-3075	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Jeff Starr Simple Ajax Chat simple-ajax-chat allows Retrieve Embedded Sensitive Data.This issue affects Simple Ajax Chat: from n/a through <= 20251121.	N/A	More Details
CVE-2026-23694	Aruba HiSpeed Cache (aruba-hispeed-cache) WordPress plugin versions prior to 3.0.5 contain a cross-site request forgery (CSRF) vulnerability affecting multiple administrative AJAX actions. The handlers for ahsc_reset_options, ahsc_debug_status, and ahsc_enable_purge perform authentication and capability checks but do not verify a WordPress nonce for state-changing requests. An attacker can induce a logged-in administrator to visit a malicious webpage that submits forged requests to admin-ajax.php, resulting in unauthorized resetting of plugin settings, toggling of the WordPress WP_DEBUG configuration, or modification of cache purging behavior without the administrator’s intent.	N/A	More Details
CVE-2025-71056	Improper session management in GCOM EPON 1GE ONU version C00R371V00B01 allows attackers to execute a session hijacking attack via spoofing the IP address of an authenticated user.	N/A	More Details
CVE-2025-70328	TOTOLINK X6000R v9.4.0cu.1498_B20250826 contains an OS command injection vulnerability in the NTPSyncWithHost handler of the /usr/sbin/shttpd executable. The host_time parameter is retrieved via sub_40C404 and passed to a date -s shell command through CsteSystem. While the first two tokens of the input are validated, the remainder of the string is not sanitized, allowing authenticated attackers to execute arbitrary shell commands via shell metacharacters.	N/A	More Details
CVE-2025-70327	TOTOLINK X5000R v9.1.0cu_2415_B20250515 contains an argument injection vulnerability in the setDiagnosisCfg handler of the /usr/sbin/lighttpd executable. The ip parameter is retrieved via websGetVar and passed to a ping command through CsteSystem without validating if the input starts with a hyphen (-). This allows remote authenticated attackers to inject arbitrary command-line options into the ping utility, potentially leading to a Denial of Service (DoS) by causing excessive resource consumption or prolonged execution.	N/A	More Details
CVE-2025-14340	Cross-site scripting in REST Management Interface in Payara Server <4.1.2.191.54, <5.83.0, <6.34.0, <7.2026.1 allows an attacker to mislead the administrator to change the admin password via URL Payload.	N/A	More Details
CVE-2025-59920	When hours are entered in time@work, version 7.0.5, it performs a query to display the projects assigned to the user. If the query URL is copied and opened in a new browser window, the ‘IDClient’ parameter is vulnerable to a blind authenticated SQL injection. If the request is made with the TWAdmin user with the sysadmin role enabled, exploiting the vulnerability will allow commands to be executed on the system; if the user does not belong to the sysadmin role, they will still be able to query data from the database.	N/A	More Details
CVE-2026-2464	Path traversal vulnerability in the AMR Printer Management 1.01 Beta web service, which allows remote attackers to read arbitrary files from the underlying Windows system by using specially crafted path traversal sequences in requests directed to the web management service. The service is accessible without authentication and runs with elevated privileges, amplifying the impact of the vulnerability. An attacker can exploit this condition to access sensitive and privileged files on the system using path traversal payloads. Successful exploitation of this vulnerability could lead to the unauthorized disclosure of internal system information, compromising the confidentiality of the affected environment.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: btrfs: reject new transactions if the fs is fully read-only [BUG] There is a bug report where a heavily fuzzed fs is mounted with all rescue mount options, which leads to the following warnings during unmount: BTRFS: Transaction aborted (error -22) Modules linked in: CPU: 0 UID: 0 PID: 9758 Comm: repro.out Not tainted 6.19.0-rc5-00002-gb71e635feefc #7 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:find_free_extent_update_loop fs/btrfs/extent-tree.c:4208 [inline] RIP: 0010:find_free_extent+0x52f0/0x5d20 fs/btrfs/extent-tree.c:4611 Call Trace: <TASK> btrfs_reserve_extent+0x2cd/0x790		

CVE-2026-23214	fs/btrfs/extent-tree.c:4705 btrfs_alloc_tree_block+0x1e1/0x10e0 fs/btrfs/extent-tree.c:5157 btrfs_force_cow_block+0x578/0x2410 fs/btrfs/ctree.c:517 btrfs_cow_block+0x3c4/0xa80 fs/btrfs/ctree.c:708 btrfs_search_slot+0xcad/0x2b50 fs/btrfs/ctree.c:2130 btrfs_truncate_inode_items+0x45d/0x2350 fs/btrfs/inode-item.c:499 btrfs_evict_inode+0x923/0xe70 fs/btrfs/inode.c:5628 evict+0x5f4/0xae0 fs/inode.c:837 __dentry_kill+0x209/0x660 fs/dcache.c:670 finish_dput+0xc9/0x480 fs/dcache.c:879 shrink_dcache_for_umount+0xa0/0x170 fs/dcache.c:1661 generic_shutdown_super+0x67/0x2c0 fs/super.c:621 kill_anon_super+0x3b/0x70 fs/super.c:1289 btrfs_kill_super+0x41/0x50 fs/btrfs/super.c:2127 deactivate_locked_super+0xbc/0x130 fs/super.c:474 cleanup_mnt+0x425/0x4c0 fs/namespace.c:1318 task_work_run+0x1d4/0x260 kernel/task_work.c:233 exit_task_work include/linux/task_work.h:40 [inline] do_exit+0x694/0x22f0 kernel/exit.c:971 do_group_exit+0x21c/0x2d0 kernel/exit.c:1112 __do_sys_exit_group kernel/exit.c:1123 [inline] __se_sys_exit_group kernel/exit.c:1121 [inline] __x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1121 x64_sys_call+0x2210/0x2210 arch/x86/include/generated/asm/syscalls_64.h:232 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe8/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x44f639 Code: Unable to access opcode bytes at 0x44f60f. RSP: 002b:00007ffc15c4e088 EFLAGS: 00000246 ORIG_RAX: 00000000000000e7 RAX: ffffffffffffffda RBX: 0000000004c32f0 RCX: 000000000044f639 RDX: 000000000000003c RSI: 00000000000000e7 RDI: 0000000000000001 RBP: 0000000000000001 R08: ffffffffffffffc0 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000004c32f0 R13: 0000000000000001 R14: 0000000000000000 R15: 0000000000000001 </TASK> Since rescue mount options will mark the full fs read-only, there should be no new transaction triggered. But during unmount we will evict all inodes, which can trigger a new transaction, and triggers warnings on a heavily corrupted fs. [CAUSE] Btrfs allows new transaction even on a read-only fs, this is to allow log replay happen even on read-only mounts, just like what ext4/xfs do. However with rescue mount options, the fs is fully read-only and cannot be remounted read-write, thus in that case we should also reject any new transactions. [FIX] If we find the fs has rescue mount options, we should treat the fs as error, so that no new transaction can be started.	N/A	More Details
CVE-2025-40986	Reflected Cross-Site Scripting (XSS) vulnerability in PideTuCita. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending him/her a malicious URL using the endpoint 'cookies/indes.php/<XSS>'. This vulnerability can be exploited to steal confidential user data, such as session cookies or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-40701	Reflected Cross-Site Scripting vulnerability in SOTESHOP, version 8.3.4. THis vulnerability allows an attacker execute JavaScript code in the victim's browser when a malicious URL with the 'id' parameter in '/adsTracker/checkAds' is sent to the victim. The vulnerability can be exploited to steal sensitive user information such as session cookies, or to perform actions on their behalf.	N/A	More Details
CVE-2025-41002	SQL injection vulnerability in Infoticketing. This vulnerability allows an unauthenticated attacker to retrieve, create, update, and delete the database by sending a POST request using the 'code' parameter in '/components/cart/cartApplyDiscount.php'.	N/A	More Details
CVE-2025-71225	In the Linux kernel, the following vulnerability has been resolved: md: suspend array while updating raid_disks via sysfs In raid1_reshape(), freeze_array() is called before modifying the r1bio memory pool (conf->r1bio_pool) and conf->raid_disks, and unfreeze_array() is called after the update is completed. However, freeze_array() only waits until nr_sync_pending and (nr_pending - nr_queued) of all buckets reaches zero. When an I/O error occurs, nr_queued is increased and the corresponding r1bio is queued to either retry_list or bio_end_io_list. As a result, freeze_array() may unblock before these r1bios are released. This can lead to a situation where conf->raid_disks and the mempool have already been updated while queued r1bios, allocated with the old raid_disks value, are later released. Consequently, free_r1bio() may access memory out of bounds in put_all_bios() and release r1bios of the wrong size to the new mempool, potentially causing issues with the mempool as well. Since only normal I/O might increase nr_queued while an I/O error occurs, suspending the array avoids this issue. Note: Updating raid_disks via ioctl SET_ARRAY_INFO already suspends the array. Therefore, we suspend the array when updating raid_disks via sysfs to avoid this issue too.	N/A	More Details
CVE-2025-71226	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: Implement settime64 as stub for MVM/MLD PTP Since commit dfb073d32cac ("ptp: Return -EINVAL on ptp_clock_register if required ops are NULL"), PTP clock registered through ptp_clock_register is required to have ptp_clock_info.settime64 set, however, neither MVM nor MLD's PTP clock implementation sets it, resulting in warnings when the interface starts up, like WARNING: drivers/ptp/ptp_clock.c:325 at ptp_clock_register+0x2c8/0x6b8, CPU#1: wpa_supplicant/469 CPU: 1 UID: 0 PID: 469 Comm: wpa_supplicant Not tainted 6.18.0+ #101 PREEMPT(full) ra: ffff800002732cd4 iwl_mvm_ptp_init+0x114/0x188 [iwlmvm] ERA: 9000000002fdc468 ptp_clock_register+0x2c8/0x6b8 iwlwifi 0000:01:00.0: Failed to register PHC clock (-22) I don't find an appropriate firmware interface to implement settime64() for iwlwifi MLD/MVM, thus instead create a stub that returns -EOPTNOTSUPP only, suppressing the warning and allowing the PTP clock to be registered.	N/A	More Details
CVE-2026-25747	Deserialization of Untrusted Data vulnerability in Apache Camel LevelDB component. The Camel-LevelDB DefaultLevelDBSerializer class deserializes data read from the LevelDB aggregation repository using java.io.ObjectInputStream without applying any ObjectInputFilter or class-loading restrictions. An attacker who can write to the LevelDB database files used by a Camel application can inject a crafted serialized Java object that, when deserialized during normal aggregation repository operations, results in arbitrary code execution in the context of the application. This issue affects Apache Camel: from 4.10.0 before 4.10.8, from 4.14.0 before 4.14.5, from 4.15.0 before 4.18.0. Users are recommended to upgrade to version 4.18.0, which fixes the issue. For the 4.10.x LTS releases, users are recommended to upgrade to 4.10.9, while for 4.14.x LTS releases, users are recommended to upgrade to 4.14.5	N/A	More Details
CVE-2025-71227	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: don't WARN for connections on invalid channels It's not clear (to me) how exactly syzbot managed to hit this, but it seems conceivable that e.g. regulatory changed and has disabled a channel between scanning (channel is checked to be usable by cfg80211_get_ies_channel_number) and connecting on the channel later. With one scenario that isn't covered elsewhere described above, the warning isn't good, replace it with a (more informative) error message.	N/A	More Details
CVE-2025-71228	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Set correct protection_map[] for VM_NONE/VM_SHARED For 32BIT platform _PAGE_PROTNONE is 0, so set a VMA to be VM_NONE or VM_SHARED will make pages non-present, then cause Oops with kernel page fault. Fix it by set correct protection_map[] for VM_NONE/VM_SHARED, replacing _PAGE_PROTNONE with _PAGE_PRESENT.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mm, swap: restore swap_space attr aviod kernel panic commit 8b47299a411a ("mm, swap: mark swap address space ro and add context debug check") made the swap address space read-only. It may lead to kernel panic if arch_prepare_to_swap returns a failure under heavy memory pressure as follows, el1_abort+0x40/0x64 el1h_64_sync_handler+0x48/0xcc el1h_64_sync+0x84/0x88 errseq_set+0x4c/0xb8 (P)		

CVE-2026-23211	__filemap_set_wb_err+0x20/0xd0 shrink_folio_list+0xc20/0x11cc evict_folios+0x1520/0x1be4 try_to_shrink_lruvec+0x27c/0x3dc shrink_one+0x9c/0x228 shrink_node+0xb3c/0xeac do_try_to_free_pages+0x170/0x4f0 try_to_free_pages+0x334/0x534 __alloc_pages_direct_reclaim+0x90/0x158 __alloc_pages_slowpath+0x334/0x588 __alloc_frozen_pages_noprof+0x224/0x2fc __folio_alloc_noprof+0x14/0x64 vma_alloc_zeroed_movable_folio+0x34/0x44 do_pte_missing+0xad4/0x1040 handle_mm_fault+0x4a4/0x790 do_page_fault+0x288/0x5f8 do_translation_fault+0x38/0x54 do_mem_abort+0x54/0xa8 Restore swap address space as not ro to avoid the panic.	N/A	More Details
CVE-2026-23212	In the Linux kernel, the following vulnerability has been resolved: bonding: annotate data-races around slave->last_rx slave->last_rx and slave->target_last_arp_rx[...] can be read and written locklessly. Add READ_ONCE() and WRITE_ONCE() annotations. syzbot reported: BUG: KCSAN: data-race in bond_rcv_validate / bond_rcv_validate write to 0xffff888149f0d428 of 8 bytes by interrupt on cpu 1: bond_rcv_validate+0x202/0x7a0 drivers/net/bonding/bond_main.c:3335 bond_handle_frame+0xde/0x5e0 drivers/net/bonding/bond_main.c:1533 __netif_receive_skb_core+0x5b1/0x1950 net/core/dev.c:6039 __netif_receive_skb_one_core net/core/dev.c:6150 [inline] __netif_receive_skb+0x59/0x270 net/core/dev.c:6265 netif_receive_skb_internal net/core/dev.c:6351 [inline] netif_receive_skb+0x4b/0x2d0 net/core/dev.c:6410 ... write to 0xffff888149f0d428 of 8 bytes by interrupt on cpu 0: bond_rcv_validate+0x202/0x7a0 drivers/net/bonding/bond_main.c:3335 bond_handle_frame+0xde/0x5e0 drivers/net/bonding/bond_main.c:1533 __netif_receive_skb_core+0x5b1/0x1950 net/core/dev.c:6039 __netif_receive_skb_one_core net/core/dev.c:6150 [inline] __netif_receive_skb+0x59/0x270 net/core/dev.c:6265 netif_receive_skb_internal net/core/dev.c:6351 [inline] netif_receive_skb+0x4b/0x2d0 net/core/dev.c:6410 br_netif_receive_skb net/bridge/br_input.c:30 [inline] NF_HOOK include/linux/netfilter.h:318 [inline] ... value changed: 0x0000000100005365 -> 0x0000000100005366	N/A	More Details
CVE-2026-23213	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Disable MMIO access during SMU Mode 1 reset During Mode 1 reset, the ASIC undergoes a reset cycle and becomes temporarily inaccessible via PCIe. Any attempt to access MMIO registers during this window (e.g., from interrupt handlers or other driver threads) can result in uncompleted PCIe transactions, leading to NMI panics or system hangs. To prevent this, set the `no_hw_access` flag to true immediately after triggering the reset. This signals other driver components to skip register accesses while the device is offline. A memory barrier `smp_mb()` is added to ensure the flag update is globally visible to all cores before the driver enters the sleep/wait state. (cherry picked from commit 7edb503fe4b6d67f47d8bb0dfafb8e699bb0f8a4)	N/A	More Details
CVE-2025-13933	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-12500. Reason: This candidate is a reservation duplicate of CVE-2025-12500. Notes: All CVE users should reference CVE-2025-12500 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-14009	A critical vulnerability exists in the NLTK downloader component of nltk/nltk, affecting all versions. The _unzip_iter function in nltk/downloader.py uses zipfile.extractall() without performing path validation or security checks. This allows attackers to craft malicious zip packages that, when downloaded and extracted by NLTK, can execute arbitrary code. The vulnerability arises because NLTK assumes all downloaded packages are trusted and extracts them without validation. If a malicious package contains Python files, such as __init__.py, these files are executed automatically upon import, leading to remote code execution. This issue can result in full system compromise, including file system access, network access, and potential persistence mechanisms.	N/A	More Details
CVE-2026-24946	Missing Authorization vulnerability in tychesoftwares Print Invoice & Delivery Notes for WooCommerce woocommerce-delivery-notes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Print Invoice & Delivery Notes for WooCommerce: from n/a through <= 5.8.0.	N/A	More Details
CVE-2026-2832	Certain Samsung MultiXpress Multifunction Printers may be vulnerable to information disclosure, potentially exposing address book entries and other device configuration information through specific APIs without proper authorization.	N/A	More Details
CVE-2026-2034	Sante DICOM Viewer Pro DCM File Parsing Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro. 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 DCM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28129.	N/A	More Details
CVE-2026-2033	MLflow Tracking Server Artifact Handler Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of MLflow Tracking Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of artifact file paths. 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 vulnerability to execute code in the context of the service account. Was ZDI-CAN-26649.	N/A	More Details
CVE-2025-15585	Fileflows versions before 25.05.2 are affected by an authenticated SQL injection vulnerability in the library-file search function. Successful exploitation requires the system to use MySQL as the underlying database and could result in privilege escalation or data exfiltration.	N/A	More Details
CVE-2026-27118	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Versions of @sveltejs/adapter-vercel prior to 6.3.2 are vulnerable to cache poisoning. An internal query parameter intended for Incremental Static Regeneration (ISR) is accessible on all routes, allowing an attacker to cause sensitive user-specific responses to be cached and served to other users. Successful exploitation requires a victim to visit an attacker-controlled link while authenticated. Existing deployments are protected by Vercel's WAF, but users should upgrade as soon as possible. This vulnerability is fixed in 6.3.2.	N/A	More Details
CVE-2026-27112	Kargo manages and automates the promotion of software artifacts. From 1.7.0 to before v1.7.8, v1.8.11, and v1.9.3, the batch resource creation endpoints of both Kargo's legacy gRPC API and newer REST API accept multi-document YAML payloads. Specially crafted payloads can manifest a bug present in the logic of both endpoints to inject arbitrary resources (of specific types only) into the underlying namespace of an existing Project using the API server's own permissions when that behavior was not intended. Critically, an attacker may exploit this as a vector for elevating their own permissions, which can then be leveraged to achieve remote code execution or secret exfiltration. Exfiltrated artifact repository credentials can be leveraged, in turn, to execute further attacks. In some configurations of the Kargo control plane's underlying Kubernetes cluster, elevated permissions may additionally be leveraged to achieve remote code execution or secret exfiltration using kubectl. This can reduce the complexity of the attack, however, worst case scenarios remain entirely achievable even without this. This	N/A	More Details

	vulnerability is fixed in v1.7.8, v1.8.11, and v1.9.3.		
CVE-2026-27111	Kargo manages and automates the promotion of software artifacts. From v1.9.0 to v1.9.2, Kargo's authorization model includes a promote verb -- a non-standard Kubernetes "dolphin verb" -- that gates the ability to advance Freight through a promotion pipeline. This verb exists to separate the ability to manage promotion-related resources from the ability to trigger promotions, enabling fine-grained access control over what is often a sensitive operation. The promote verb is correctly enforced in Kargo's legacy gRPC API. However, three endpoints in the newer REST API omit this check, relying only on standard Kubernetes RBAC for the underlying resource operations (patch on freights/status or create on promotions). This permits users who hold those standard permissions -- but who were deliberately not granted promote -- to bypass the intended authorization boundary. The affected endpoints are /v1beta1/projects/{project}/freight/{freight}/approve, /v1beta1/projects/{project}/stages/{stage}/promotions, and /v1beta1/projects/{project}/stages/{stage}/promotions/downstream. This vulnerability is fixed in v1.9.3.	N/A	More Details
CVE-2026-0797	GIMP ICO File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. 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 ICO 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-28599.	N/A	More Details
CVE-2026-0777	Xmind Attachment Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Xmind. 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 handling of attachments. When opening an attachment, the user interface fails to warn the user of unsafe actions. An attacker can leverage this vulnerability to execute code in the context of current user. Was ZDI-CAN-26034.	N/A	More Details
CVE-2026-27020	Photobooth prior to 1.0.1 has a cross-site scripting (XSS) vulnerability in user input fields. Malicious users could inject scripts through unvalidated form inputs. This vulnerability is fixed in 1.0.1.	N/A	More Details
CVE-2026-2473	Predictable bucket naming in Vertex AI Experiments in Google Cloud Vertex AI from version 1.21.0 up to (but not including) 1.133.0 on Google Cloud Platform allows an unauthenticated remote attacker to achieve cross-tenant remote code execution, model theft, and poisoning via pre-creating predictably named Cloud Storage buckets (Bucket Squatting). This vulnerability was patched and no customer action is needed.	N/A	More Details
CVE-2026-2472	Stored Cross-Site Scripting (XSS) in the _genai/_evals_visualization component of Google Cloud Vertex AI SDK (google-cloud-aiplatform) versions from 1.98.0 up to (but not including) 1.131.0 allows an unauthenticated remote attacker to execute arbitrary JavaScript in a victim's Jupyter or Colab environment via injecting script escape sequences into model evaluation results or dataset JSON data.	N/A	More Details
CVE-2026-2333	Improper Neutralization of Special Elements used in a Command ('Command Injection') in Owl opds 2.2.0.4 allows Command Injection via a crafted network request.	N/A	More Details
CVE-2026-2036	GFI Archiver MArc.Store Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the configuration of the MArc.Store.Remoting.exe process. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-27936.	N/A	More Details
CVE-2026-26102	Incorrect Permission Assignment for Critical Resource in Owl opds 2.2.0.4 allows File Manipulation via a crafted network request.	N/A	More Details
CVE-2026-26101	Incorrect Permission Assignment for Critical Resource in Owl opds 2.2.0.4 allows File Manipulation via a crafted network request.	N/A	More Details
CVE-2026-26100	Incorrect Permission Assignment for Critical Resource in Owl opds 2.2.0.4 allows File Manipulation via a crafted network request.	N/A	More Details
CVE-2026-26099	Uncontrolled Search Path Element in Owl opds 2.2.0.4 allows Leveraging/Manipulating Configuration File Search Paths via a crafted network request.	N/A	More Details
CVE-2026-26098	Uncontrolled Search Path Element in Owl opds 2.2.0.4 allows Leveraging/Manipulating Configuration File Search Paths via a crafted network request.	N/A	More Details
CVE-2026-26097	Uncontrolled Search Path Element in Owl opds 2.2.0.4 allows Leveraging/Manipulating Configuration File Search Paths via a crafted network request.	N/A	More Details
CVE-2026-26096	Incorrect Permission Assignment for Critical Resource in Owl opds 2.2.0.4 allows File Manipulation via a crafted network request.	N/A	More Details
CVE-2026-26095	Incorrect Permission Assignment for Critical Resource in Owl opds 2.2.0.4 allows File Manipulation via a crafted network request.	N/A	More Details

CVE-2026-26093	Improper Neutralization of Special Elements used in a Command ('Command Injection') in Owl opds 2.2.0.4 allows Command Injection via a crafted network request.	N/A	More Details
CVE-2026-1842	HyperCloud versions 2.3.5 through 2.6.8 improperly allowed refresh tokens to be used directly for resource access and failed to invalidate previously issued access tokens when a refresh token was used. Because refresh tokens have a significantly longer lifetime (default one year), an authenticated client could use a refresh token in place of an access token to maintain long-term access without token rotation. Additionally, old access tokens remained valid after refresh, enabling concurrent or extended use beyond intended session boundaries. This vulnerability could allow prolonged unauthorized access if a token is disclosed.	N/A	More Details
CVE-2026-24953	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mitchell Bennis Simple File List simple-file-list allows Path Traversal.This issue affects Simple File List: from n/a through <= 6.1.15.	N/A	More Details
CVE-2026-2035	Deciso OPNsense diag_backup.php filename Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Deciso OPNsense. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of backup configuration files. 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 execute code in the context of root. Was ZDI-CAN-28131.	N/A	More Details
CVE-2026-2037	GFI Archiver MArc.Core Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the configuration of the MArc.Core.Remoting.exe process, which listens on port 8017. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-27935.	N/A	More Details
CVE-2026-27452	ASN.1 TypeScript ESM library, including codecs for Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). In versions 11.0.5 and below, in some cases, decoding an INTEGER could leak the underlying ArrayBuffer. This issue is expected to be fixed in version 11.0.6.	N/A	More Details
CVE-2026-27192	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. In versions 5.0.39 and below, origin validation uses startsWith() for comparison, allowing attackers to bypass the check by registering a domain that shares a common prefix with an allowed origin.The getAllowedOrigin() function checks if the Referer header starts with any allowed origin, and this comparison is insufficient as it only validates the prefix. This is exploitable when the origins array is configured and an attacker registers a domain starting with an allowed origin string (e.g., https://target.com.attacker.com bypasses https://target.com). On its own, tokens are still redirected to a configured origin. However, in specific scenarios an attacker can initiate the OAuth flow from an unauthorized origin and exfiltrate tokens, achieving full account takeover. This issue has bee fixed in version 5.0.40.	N/A	More Details
CVE-2026-27210	Pannellum is a lightweight, free, and open source panorama viewer for the web. In versions 3.5.0 through 2.5.6, the hot spot attributes configuration property allowed any attribute to be set, including HTML event handler attributes, allowing for potential XSS attacks. This affects websites hosting the standalone viewer HTML file and any other use of untrusted JSON config files (bypassing the protections of the escapeHTML parameter). As certain events fire without any additional user interaction, visiting a standalone viewer URL that points to a malicious config file — without additional user interaction — is sufficient to trigger the vulnerability and execute arbitrary JavaScript code, which can, for example, replace the contents of the page with arbitrary content and make it appear to be hosted by the website hosting the standalone viewer HTML file. This issue has been fixed in version 2.5.7. To workaround, setting the Content-Security-Policy header to script-src-attr 'none' will block execution of inline event handlers, mitigating this vulnerability. Don't host pannellum.htm on a domain that shares cookies with user authentication to mitigate XSS risk.	N/A	More Details
CVE-2026-27199	Werkzeug is a comprehensive WSGI web application library. Versions 3.1.5 and below, the safe_join function allows Windows device names as filenames if preceded by other path segments. This was previously reported as GHSA-hgf8-39gv-g3f2, but the added filtering failed to account for the fact that safe_join accepts paths with multiple segments, such as example/NUL. The function send_from_directory uses safe_join to safely serve files at user-specified paths under a directory. If the application is running on Windows, and the requested path ends with a special device name, the file will be opened successfully, but reading will hang indefinitely. This issue has been fixed in version 3.1.6.	N/A	More Details
CVE-2026-27534	Rejected reason: Not used	N/A	More Details
CVE-2026-27533	Rejected reason: Not used	N/A	More Details
CVE-2026-27532	Rejected reason: Not used	N/A	More Details
CVE-2026-27531	Rejected reason: Not used	N/A	More Details
CVE-2026-27530	Rejected reason: Not used	N/A	More Details
CVE-2026-27529	Rejected reason: Not used	N/A	More Details

CVE-2026-27528	Rejected reason: Not used	N/A	More Details
CVE-2026-27527	Rejected reason: Not used	N/A	More Details
CVE-2026-27193	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. In versions 5.0.39 and below, all HTTP request headers are stored in the session cookie, which is signed but not encrypted, exposing internal proxy/gateway headers to clients. The OAuth service stores the complete headers object in the session, then the session is persisted using cookie-session, which base64-encodes the data. While the cookie is signed to prevent tampering, the contents are readable by anyone by simply decoding the base64 value. Under specific deployment configurations (e.g., behind reverse proxies or API gateways), this can lead to exposure of sensitive internal infrastructure details such as API keys, service tokens, and internal IP addresses. This issue has been fixed in version 5.0.40.	N/A	More Details
CVE-2026-27191	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. Versions 5.0.39 and below the redirect query parameter is appended to the base origin without validation, allowing attackers to steal access tokens via URL authority injection. This leads to full account takeover, as the attacker obtains the victim's access token and can impersonate them. The application constructs the final redirect URL by concatenating the base origin with the user-supplied redirect parameter. This is exploitable when the origins array is configured and origin values do not end with /. An attacker can supply @attacker.com as the redirect value results in https://target.com@attacker.com#access_token=..., where the browser interprets attacker.com as the host, leading to full account takeover. This issue has been fixed in version 5.0.40.	N/A	More Details
CVE-2026-2040	PDF-XChange Editor TrackerUpdate Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of PDF-XChange Editor. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the TrackerUpdate process. The product loads a library from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of a target user. Was ZDI-CAN-27788.	N/A	More Details
CVE-2025-12811	Improper Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') in Delinea Inc. Cloud Suite and Privileged Access Service. If you're not using the latest Server Suite agents, this fix requires that you upgrade to Server Suite 2023.1 (agent 6.0.1) or later. * If you cannot upgrade to Release 2023.1 (agent version 6.0.1) or later, you can choose one of the following versions: * Server Suite release 2023.0.5 (agent version 6.0.0-158) * Server Suite release 2022.1.10 (agent version 5.9.1-337)	N/A	More Details
CVE-2025-12812	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in Delinea Inc. Cloud Suite and Privileged Access Service. Remediation: This issue is fixed in Cloud Suite: 25.1	N/A	More Details
CVE-2025-15581	Orthanc versions before 1.12.10 are affected by an authorisation logic flaw in the application's HTTP Basic Authentication implementation. Successful exploitation could result in Privilege Escalation, potentially allowing full administrative access.	N/A	More Details
CVE-2026-2635	MLflow Use of Default Password Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of MLflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the basic_auth.ini file. The file contains hard-coded default credentials. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of the administrator. Was ZDI-CAN-28256.	N/A	More Details
CVE-2026-2492	TensorFlow HDF5 Library Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of TensorFlow. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of plugins. The application loads plugins from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of a target user. Was ZDI-CAN-25480.	N/A	More Details
CVE-2026-2490	RustDesk Client for Windows Transfer File Link Following Information Disclosure Vulnerability. This vulnerability allows local attackers to disclose sensitive information on affected installations of RustDesk Client for Windows. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Transfer File feature. By uploading a symbolic link, an attacker can abuse the service to read arbitrary files. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-27909.	N/A	More Details
CVE-2026-2048	GIMP XWD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. 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 XWD 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28591.	N/A	More Details
CVE-2026-2047	GIMP ICNS File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. 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 ICNS 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-28530.	N/A	More Details
CVE-2026-2045	GIMP XWD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. 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 XWD 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28265.	N/A	More Details
CVE-	GIMP PGM File Parsing Uninitialized Memory Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the		More

2026-2044	target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PGM files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28158.	N/A	Details
CVE-2025-71250	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-26351	GetSimpleCMS Community Edition (CE) version 3.3.16 contains a stored cross-site scripting (XSS) vulnerability in the Theme to Components functionality within components.php. User-supplied input provided to the "slug" field of a component is stored without proper output encoding. While other fields are sanitized using safe_slash_html(), the slug parameter is written to XML and later rendered in the administrative interface without sanitation, resulting in persistent execution of arbitrary JavaScript. An authenticated administrator can inject malicious script content that executes whenever the affected Components page is viewed by any authenticated user, enabling session hijacking, unauthorized administrative actions, and persistent compromise of the CMS administrative interface.	N/A	More Details