SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 07 January 2026

Generated on 07 January 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-2025-30996	Unrestricted Upload of File with Dangerous Type vulnerability in Themify Themify Sidepane WordPress Theme, Themify Themify Newsy, Themify Themify Folo, Themify Themify Edmin, Themify Bloggie, Themify Photobox, Themify Wigi, Themify Rezo, Themify Slide allows Upload a Web Shell to a Web Server.This issue affects Themify Sidepane WordPress Theme: from n/a through 1.9.8; Themify Newsy: from n/a through 1.9.9; Themify Folo: from n/a through 1.9.6; Themify Edmin: from n/a through 2.0.0; Bloggie: from n/a through 2.0.8; Photobox: from n/a through 2.0.1; Wigi: from n/a through 2.0.1; Rezo: from n/a through 1.9.7; Slide: from n/a through 1.7.5.	9.9	More Details
CVE-2025-64420	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions prior to and including v4.0.0-beta.434, low privileged users are able to see the private key of the root user on the Coolify instance. This allows them to ssh to the server and authenticate as root user, using the private key. As of time of publication, it is unclear if a patch is available.	9.9	More Details
CVE-2025-31048	Unrestricted Upload of File with Dangerous Type vulnerability in Themify Shopo allows Upload a Web Shell to a Web Server.This issue affects Shopo: from n/a through 1.1.4.	9.9	More Details
CVE-2025-59157	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.420.7, the Git Repository field during project creation is vulnerable to command injection. User input is not properly sanitized, allowing attackers to inject arbitrary shell commands that execute on the underlying server during the deployment workflow. A regular member user can exploit this vulnerability. Version 4.0.0-beta.420.7 contains a patch for the issue.	9.9	More Details

CVE-2025-60534	Blue Access Cobalt v02.000.195 suffers from an authentication bypass vulnerability, which allows an attacker to selectively proxy requests in order to operate functionality on the web application without the need to authenticate with legitimate credentials.	9.8	More Details
CVE-2025-39477	Missing Authorization vulnerability in Sfwebservice InWave Jobs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects InWave Jobs: from n/a through 3.5.8.	9.8	More Details
CVE-2025-65212	An issue was discovered in NJHYST HY511 POE core before 2.1 and plugins before 0.1. The vulnerability stems from the device's insufficient cookie verification, allowing an attacker to directly request the configuration file address and download the core configuration file without logging into the device management backend. By reading the corresponding username and self-decrypted MD5 password in the core configuration file, the attacker can directly log in to the backend, thereby bypassing the front-end backend login page.	9.8	More Details
CVE-2025-60262	An issue in H3C M102G HM1A0V200R010 wireless controller and BA1500L SWBA1A0V100R006 wireless access point, there is a misconfiguration vulnerability about vsftpd. Through this vulnerability, all files uploaded anonymously via the FTP protocol is automatically owned by the root user and remote attackers could gain root-level control over the devices.	9.8	More Details
CVE-2020-36925	Arteco Web Client DVR/NVR contains a session hijacking vulnerability with insufficient session ID complexity that allows remote attackers to bypass authentication. Attackers can brute force session IDs within a specific numeric range to obtain valid sessions and access live camera streams without authorization.	9.8	More Details
CVE-2020-36923	Sony BRAVIA Digital Signage 1.7.8 contains an insecure direct object reference vulnerability that allows attackers to bypass authorization controls. Attackers can access hidden system resources like '/#/content-creation' by manipulating client-side access restrictions.	9.8	More Details
CVE-2020-36912	Plexus anblick Digital Signage Management 3.1.13 contains an open redirect vulnerability in the 'PantallaLogin' script that allows attackers to manipulate the 'pagina' GET parameter. Attackers can craft malicious links that redirect users to arbitrary websites by exploiting improper input validation in the parameter.	9.8	More Details
CVE-2025-15001	The FS Registration Password plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.1. 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-2025-14996	The AS Password Field In Default Registration Form plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. 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-2026-21675	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below contain a Use After Free vulnerability in the CIccXform::Create() function, where it deletes the hint. This issue is fixed in version 2.3.1.1.	9.8	More Details
CVE-2025-15385	Insufficient Verification of Data Authenticity vulnerability in TECNO Mobile com.Afmobi.Boomplayer allows Authentication Bypass.This issue affects com.Afmobi.Boomplayer: 7.4.63.	9.8	More Details

CVE-2025-15444	Crypt::Sodium::XS module versions prior to 0.000042, for Perl, include a vulnerable version of libsodium libsodium <= 1.0.20 or a version of libsodium released before December 30, 2025 contains a vulnerability documented as CVE-2025-69277 https://www.cve.org/CVERecord?id=CVE-2025-69277 . The libsodium vulnerability states: In atypical use cases involving certain custom cryptography or untrusted data to crypto_core_ed25519_is_valid_point, mishandles checks for whether an elliptic curve point is valid because it sometimes allows points that aren't in the main cryptographic group. 0.000042 includes a version of libsodium updated to 1.0.20-stable, released January 3, 2026, which includes a fix for the vulnerability.	9.8	More Details
CVE-2025-69286	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In versions prior to 0.22.0, the use of an insecure key generation algorithm in the API key and beta (assistant/agent share auth) token generation process allows these tokens to be mutually derivable. Specifically, both tokens are generated using the same `URLSafeTimedSerializer` with predictable inputs, enabling an unauthorized user who obtains the shared assistant/agent URL to derive the personal API key. This grants them full control over the assistant/agent owner's account. Version 0.22.0 fixes the issue.	9.8	More Details
CVE-2025-14346	WHILL Model C2 Electric Wheelchairs and Model F Power Chairs do not enforce authentication for Bluetooth connections. An attacker within range can pair with the device and issue movement commands, override speed restrictions, and manipulate configuration profiles without any credentials or user interaction.	9.8	More Details
CVE-2025-15029	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Centreon Infra Monitoring (Awie export modules) allows SQL Injection to unauthenticated user. This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.3, from 24.04.0 before 24.04.3.	9.8	More Details
CVE-2025-15026	Missing Authentication for Critical Function vulnerability in Centreon Infra Monitoring centreon-awie (Awie import module) allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.3, from 24.04.0 before 24.04.3.	9.8	More Details
CVE-2025-67268	gpsd before commit dc966aa contains a heap-based out-of-bounds write vulnerability in the drivers/driver_nmea2000.c file. The hnd_129540 function, which handles NMEA2000 PGN 129540 (GNSS Satellites in View) packets, fails to validate the user-supplied satellite count against the size of the skyview array (184 elements). This allows an attacker to write beyond the bounds of the array by providing a satellite count up to 255, leading to memory corruption, Denial of Service (DoS), and potentially arbitrary code execution.	9.8	More Details
CVE-2025-65125	SQL injection in gosaliajainam/online-movie-booking 5.5 in movie_details.php allows attackers to gain sensitive information.	9.8	More Details
CVE-2025-14998	The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.24. 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-2025-64419	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.445, parameters coming from docker-compose.yaml are not sanitized when used in commands. If a victim user creates an application from an attacker repository (using build pack "docker compose"), the attacker can execute commands on the Coolify instance as root. Version 4.0.0-beta.445 fixes the issue.	9.6	More Details
	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.19.0, an unauthenticated attacker can pollute the internal state		

CVE-2025-66398	(`restoreFilePath`) of the server via the `/skServer/validateBackup` endpoint. This allows the attacker to hijack the administrator's "Restore" functionality to overwrite critical server configuration files (e.g., `security.json`, `package.json`), leading to account takeover and Remote Code Execution (RCE). Version 2.19.0 patches this vulnerability.	9.6	More Details
CVE-2025-39484	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Waituk Entrada allows SQL Injection.This issue affects Entrada: from n/a through 5.7.7.	9.3	More Details
CVE-2025-68865	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Infility Infility Global allows SQL Injection.This issue affects Infility Global: from n/a through 2.14.48.	9.3	More Details
CVE-2025-30633	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Amazon Native Shopping Recommendations allows SQL Injection.This issue affects Amazon Native Shopping Recommendations: from n/a through 1.3.	9.3	More Details
CVE-2025-67397	An issue in Passy v.1.6.3 allows a remote authenticated attacker to execute arbitrary commands via a crafted HTTP request using a specific payload injection.	9.1	More Details
CVE-2025-69288	Titra is open source project time tracking software. Prior to version 0.99.49, Titra allows any authenticated Admin user to modify the timeEntryRule in the database. The value is then passed to a NodeVM value to execute as code. Without sanitization, it leads to a Remote Code Execution. Version 0.99.49 fixes the issue.	9.1	More Details
CVE-2023-50897	Unrestricted Upload of File with Dangerous Type vulnerability in Meow Apps Media File Renamer allows Using Malicious Files.This issue affects Media File Renamer: from n/a through 5.7.7.	9.1	More Details
CVE-2025-68620	Signal K Server is a server application that runs on a central hub in a boat. Versions prior to 2.19.0 expose two features that can be chained together to steal JWT authentication tokens without any prior authentication. The attack combines WebSocket-based request enumeration with unauthenticated polling of access request status. The first is Unauthenticated WebSocket Request Enumeration: When a WebSocket client connects to the SignalK stream endpoint with the `serverevents=all` query parameter, the server sends all cached server events including `ACCESS_REQUEST` events that contain details about pending access requests. The `startServerEvents` function iterates over `app.lastServerEvents` and writes each cached event to any connected client without verifying authorization level. Since WebSocket connections are allowed for readonly users (which includes unauthenticated users when `allow_readonly` is true), attackers receive these events containing request IDs, client identifiers, descriptions, requested permissions, and IP addresses. The second is Unauthenticated Token Polling: The access request status endpoint at `/signalk/v1/access/requests/:id` returns the full state of an access request without requiring authentication. When an administrator approves a request, the response includes the issued JWT token in plaintext. The `queryRequest` function returns the complete request object including the token field, and the REST endpoint uses readonly authentication, allowing unauthenticated access. An attacker has two paths to exploit these vulnerabilities. Either the attacker creates their own access request (using the IP spoofing vulnerability to craft a convincing spoofed request), then polls their own request ID until an administrator approves it, receiving the JWT token; or the attacker passively monitors the WebSocket stream to discover request IDs from legitimate devices, then polls those IDs and steals the JWT tokens when administrators approve them, hijacking legitimate device credentials. Both paths require zero authentication and enable complete authentication bypass. Version 2.19.0 fixes the underlying issues.	9.1	More Details
CVE-	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and		

2025-27807	Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 9110, W920, W930, W1000, Modem 5123, Modem 5300, Modem 5400. The lack of a length check leads to out-of-bounds writes via malformed NAS packets.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-15431	A flaw has been found in UTT 进取 512W 1.7.7-171114. This affects the function strcpy of the file /goform/formFtpServerDirConfig. Executing manipulation of the argument filename can lead to buffer overflow. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2020-36916	TDM Digital Signage PC Player 4.1.0.4 contains an elevation of privileges vulnerability that allows authenticated users to modify executable files. Attackers can leverage the 'Modify' permissions for authenticated users to replace executable files with malicious binaries and gain elevated system access.	8.8	More Details
CVE-2025-15240	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has an Arbitrary File Upload vulnerability, allowing authenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	8.8	More Details
CVE-2025-15462	A vulnerability has been found in UTT 进取 520W 1.7.7-180627. This issue affects the function strcpy of the file /goform/ConfigAdvideo. The manipulation of the argument timestart leads to buffer overflow. 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.	8.8	More Details
CVE-2025-15461	A flaw has been found in UTT 进取 520W 1.7.7-180627. This vulnerability affects the function strcpy of the file /goform/formTaskEdit. Executing a manipulation of the argument selDateType can lead to buffer overflow. 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.	8.8	More Details
CVE-2025-15460	A vulnerability was detected in UTT 进取 520W 1.7.7-180627. This affects the function strcpy of the file /goform/formPptpClientConfig. Performing a manipulation of the argument EncryptionMode results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-15459	A security vulnerability has been detected in UTT 进取 520W 1.7.7-180627. Affected by this issue is the function strcpy of the file /goform/formUser. Such manipulation of the argument passwd1 leads to buffer overflow. 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.	8.8	More Details
CVE-2026-21677	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below have Undefined Behavior in its CIccCLUT::Init function which initializes and sets the size of a CLUT. This issue is fixed in version 2.3.1.1.	8.8	More Details
CVE-2026-21676	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below have a Heap-based Buffer Overflow in its CIccMBB::Validate function which checks tag data validity. This issue is fixed in version 2.3.1.1.	8.8	More Details
CVE-2025-29004	Incorrect Privilege Assignment vulnerability in AA-Team Premium Age Verification / Restriction for WordPress, AA-Team Responsive Coming Soon Landing Page / Holding Page for WordPress allows Privilege Escalation.This issue affects Premium Age Verification / Restriction for WordPress: from n/a through 3.0.2; Responsive Coming	8.8	More Details

	Soon Landing Page / Holding Page for WordPress: from n/a through 3.0.		
CVE-2025-15387	VPN Firewall developed by QNO Technology has a Insufficient Entropy vulnerability, allowing unauthenticated remote attackers to obtain any logged-in user session through brute-force attacks and subsequently log into the system.	8.8	More Details
CVE-2025-15388	VPN Firewall developed by QNO Technology has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	8.8	More Details
CVE-2026-0640	A weakness has been identified in Tenda AC23 16.03.07.52. This affects the function sscanf of the file /goform/PowerSaveSet. Executing a manipulation of the argument Time can lead to buffer overflow. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2025-31047	Deserialization of Untrusted Data vulnerability in Themify Themify Edmin allows Object Injection.This issue affects Themify Edmin: from n/a through 2.0.0.	8.8	More Details
CVE-2025-47553	Deserialization of Untrusted Data vulnerability in Digital zoom studio DZS Video Gallery allows Object Injection.This issue affects DZS Video Gallery: from n/a through 12.25.	8.8	More Details
CVE-2020-36920	iDS6 DSSPro Digital Signage System 6.2 contains an improper access control vulnerability that allows authenticated users to elevate privileges through console JavaScript functions. Attackers can create users, modify roles and permissions, and potentially achieve full application takeover by exploiting insecure direct object references.	8.8	More Details
CVE-2020-36910	Cayin Signage Media Player 3.0 contains an authenticated remote command injection vulnerability in system.cgi and wizard_system.cgi pages. Attackers can exploit the 'NTP_Server_IP' parameter with default credentials to execute arbitrary shell commands as root.	8.8	More Details
CVE-2025-15389	VPN Firewall developed by QNO Technology has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	8.8	More Details
CVE-2025-15430	A vulnerability was detected in UTT 进取 512W 1.7.7-171114. Affected by this issue is the function strcpy of the file /goform/formFtpServerShareDirSelcet. Performing manipulation of the argument oldfilename results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-15428	A weakness has been identified in UTT 进取 512W 1.7.7-171114. Affected is the function strcpy of the file /goform/formRemoteControl. This manipulation of the argument Profile causes 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. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-55204	muffon is a cross-platform music streaming client for desktop. Versions prior to 2.3.0 have a one-click Remote Code Execution (RCE) vulnerability in. An attacker can exploit this issue by embedding a specially crafted `muffon://` link on any website they control. When a victim visits the site or clicks the link, the browser triggers Muffon’s custom URL handler, causing the application to launch and process the URL. This leads to RCE on the victim's machine without further interaction. Version 2.3.0 patches the issue.	8.8	More Details
CVE-2026-21633	A malicious actor with access to the adjacent network could obtain unauthorized access to a UniFi Protect Camera by exploiting a discovery protocol vulnerability in the Unifi Protect Application (Version 6.1.79 and earlier). Affected Products: UniFi Protect Application (Version 6.1.79 and earlier). Mitigation: Update your UniFi Protect Application to Version 6.2.72 or later.	8.8	More Details

CVE-2025-15429	A security vulnerability has been detected in UTT 进取 512W 1.7.7-171114. Affected by this vulnerability is the function strcpy of the file /goform/formConfigCliForEngineerOnly. Such manipulation of the argument addCommand leads to buffer overflow. 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.	8.8	More Details
CVE-2025-68700	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In versions prior to 0.23.0, a low-privileged authenticated user (normal login account) can execute arbitrary system commands on the server host process via the frontend Canvas CodeExec component, completely bypassing sandbox isolation. This occurs because untrusted data (stdout) is parsed using eval() with no filtering or sandboxing. The intended design was to "automatically convert string results into Python objects," but this effectively executes attacker-controlled code. Additional endpoints lack access control or contain inverted permission logic, significantly expanding the attack surface and enabling chained exploitation. Version 0.23.0 contains a patch for the issue.	8.8	More Details
CVE-2021-47742	Epic Games Psyonix Rocket League <=1.95 contains an insecure permissions vulnerability that allows authenticated users to modify executable files with full access permissions. Attackers can leverage the 'F' (Full) flag for the 'Authenticated Users' group to change executable files and potentially escalate system privileges.	8.8	More Details
CVE-2021-47745	Cypress Solutions CTM-200 2.7.1 contains an authenticated command injection vulnerability in the firmware upgrade script that allows remote attackers to execute shell commands. Attackers can exploit the 'fw_url' parameter in the ctm-config-upgrade.sh script to inject and execute arbitrary commands with root privileges.	8.8	More Details
CVE-2021-47747	meterN 1.2.3 contains an authenticated remote code execution vulnerability in admin_meter2.php and admin_indicator2.php scripts. Attackers can exploit the 'COMMANDx' and 'LIVECOMMANDx' POST parameters to execute arbitrary system commands with administrative privileges.	8.8	More Details
CVE-2026-21485	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below are prone to have Undefined Behavior (UB) and Out of Memory errors. This issue is fixed in version 2.3.1.2.	8.8	More Details
CVE-2025-14124	The Team WordPress plugin before 5.0.11 does not properly sanitize and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	8.6	More Details
CVE-2025-68044	Authorization Bypass Through User-Controlled Key vulnerability in Rustaurius Five Star Restaurant Reservations allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Five Star Restaurant Reservations: from n/a through 2.7.8.	8.6	More Details
CVE-2025-69414	Plex Media Server (PMS) through 1.42.2.10156 allows retrieval of a permanent access token via a /myplex/account call with a transient access token.	8.5	More Details
CVE-2025-31044	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Premium SEO Pack allows SQL Injection.This issue affects Premium SEO Pack: from n/a through 3.3.2.	8.5	More Details
CVE-2025-28949	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Codedraft Mediabay - WordPress Media Library Folders allows Blind SQL Injection.This issue affects Mediabay - WordPress Media Library Folders: from n/a through 1.4.	8.5	More Details
CVE-2025-	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer) allows SQL Injection.This issue affects Amazon Affiliates Addon for	8.5	More Details

30628	WPBakery Page Builder (formerly Visual Composer): from n/a through 1.2.		
CVE-2025-49495	An issue was discovered in the WiFi driver in Samsung Mobile Processor Exynos 1380, 1480, 2400, 1580. Mishandling of an NL80211 vendor command leads to a buffer overflow.	8.4	More Details
CVE-2025-53966	An issue was discovered in Samsung Mobile Processor Exynos 1380, 1480, 2400, and 1580. Incorrect Handling of the NL80211 vendor command leads to a buffer overflow during handling of an IOCTL message.	8.4	More Details
CVE-2020-36903	Selea CarPlateServer 4.0.1.6 contains an unquoted service path vulnerability in the Windows service configuration that allows local users to potentially execute code with elevated privileges. Attackers can exploit the service's unquoted binary path by inserting malicious code in the system root path that could execute with LocalSystem privileges during application startup or reboot.	8.4	More Details
CVE-2025-69087	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes FreeAgent allows PHP Local File Inclusion.This issue affects FreeAgent: from n/a through 2.1.2.	8.1	More Details
CVE-2025-47411	A user with a legitimate non-administrator account can exploit a vulnerability in the user ID creation mechanism in Apache StreamPipes that allows them to swap the username of an existing user with that of an administrator. This vulnerability allows an attacker to gain administrative control over the application by manipulating JWT tokens, which can lead to data tampering, unauthorized access and other security issues. This issue affects Apache StreamPipes: through 0.97.0. Users are recommended to upgrade to version 0.98.0, which fixes the issue.	8.1	More Details
CVE-2025-52863	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.0.3192 build 20250716 and later	8.1	More Details
CVE-2025-65110	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. Prior to versions 6.1.2 and 5.6.3, applications meeting two conditions are at risk of arbitrary JavaScript code execution, even if "safe mode" expressionInterpreter is used. First, they use \`vega\` in an application that attaches both \`vega\` library and a \`vega.View\` instance similar to the Vega Editor to the global \`window\`, or has any other satisfactory function gadgets in the global scope. Second, they allow user-defined Vega \`JSON\` definitions (vs JSON that was is only provided through source code). This vulnerability allows for DOM XSS, potentially stored, potentially reflected, depending on how the library is being used. The vulnerability requires user interaction with the page to trigger. An attacker can exploit this issue by tricking a user into opening a malicious Vega specification. Successful exploitation allows the attacker to execute arbitrary JavaScript in the context of the application’s domain. This can lead to theft of sensitive information such as authentication tokens, manipulation of data displayed to the user, or execution of unauthorized actions on behalf of the victim. This exploit compromises confidentiality and integrity of impacted applications.Patched versions are available in \`vega-selections@6.1.2\` (requires ESM) for Vega v6 and \`vega-selections@5.6.3\` (no ESM needed) for Vega v5. As a workaround, do not attach \`vega\` or \`vega.View\` instances to global variables or the window as the editor used to do. This is a development-only debugging practice that should not be used in any situation where Vega/Vega-lite definitions can come from untrusted parties.	8.1	More Details
CVE-	Use After Free vulnerability was discovered in fs/vfs/fs_rename code of the Apache NuttX RTOS, that due recursive implementation and single buffer use by two different pointer variables allowed arbitrary user provided size buffer reallocation and write to the previously freed heap chunk, that in specific cases could cause unintended virtual		

2025-48769	filesystem rename/move operation results. This issue affects Apache NuttX RTOS: from 7.20 before 12.11.0. Users of virtual filesystem based services with write access especially when exposed over the network (i.e. FTP) are affected and recommended to upgrade to version 12.11.0 that fixes the issue.	8.1	More Details
CVE-2025-32304	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mojoomla WPCHURCH allows PHP Local File Inclusion.This issue affects WPCHURCH: from n/a through 2.7.0.	8.1	More Details
CVE-2025-52864	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.0.3192 build 20250716 and later	8.1	More Details
CVE-2025-52872	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.0.3192 build 20250716 and later	8.1	More Details
CVE-2025-69083	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Frappé allows PHP Local File Inclusion.This issue affects Frappé: from n/a through 1.8.	8.1	More Details
CVE-2025-69086	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Jwsthemes Issabella allows PHP Local File Inclusion.This issue affects Issabella: from n/a through 1.1.2.	8.1	More Details
CVE-2025-61916	Spinnaker is an open source, multi-cloud continuous delivery platform. Versions prior to 2025.1.6, 2025.2.3, and 2025.3.0 are vulnerable to server-side request forgery. The primary impact is allowing users to fetch data from a remote URL. This data can be then injected into spinnaker pipelines via helm or other methods to extract things LIKE idmsv1 authentication data. This also includes calling internal spinnaker API's via a get and similar endpoints. Further, depending upon the artifact in question, auth data may be exposed to arbitrary endpoints (e.g. GitHub auth headers) leading to credentials exposure. To trigger this, a spinnaker installation MUST have two things. The first is an artifact enabled that allows user input. This includes GitHub file artifacts, BitBucket, GitLab, HTTP artifacts and similar artifact providers. JUST enabling the http artifact provider will add a "no-auth" http provider that could be used to extract link local data (e.g. AWS Metadata information). The second is a system that can consume the output of these artifacts. e.g. Rosco helm can use this to fetch values data. K8s account manifests if the API returns JSON can be used to inject that data into the pipeline itself though the pipeline would fail. This vulnerability is fixed in versions 2025.1.6, 2025.2.3, and 2025.3.0. As a workaround, disable HTTP account types that allow user input of a given URL. This is probably not feasible in most cases. Git, Docker and other artifact account types with explicit URL configurations bypass this limitation and should be safe as they limit artifact URL loading. Alternatively, use one of the various vendors which provide OPA policies to restrict pipelines from accessing or saving a pipeline with invalid URLs.	7.9	More Details
CVE-2025-14026	Forcepoint One DLP Client, version 23.04.5642 (and possibly newer versions), includes a restricted version of Python 2.5.4 that prevents use of the ctypes library. ctypes is a foreign function interface (FFI) for Python, enabling calls to DLLs/shared libraries, memory allocation, and direct code execution. It was demonstrated that these restrictions could be bypassed.	7.8	More Details
CVE-	In display, there is a possible out of bounds write due to a missing bounds check. This		

2025-20778	could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184870; Issue ID: MSV-4729.	7.8	More Details
CVE-2025-20780	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184061; Issue ID: MSV-4712.	7.8	More Details
CVE-2026-21486	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below contain Use After Free, Heap-based Buffer Overflow and Integer Overflow or Wraparound and Out-of-bounds Write vulnerabilities in its CIccSparseMatrix::CIccSparseMatrix function. This issue is fixed in version 2.3.1.2.	7.8	More Details
CVE-2025-20795	In KeyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10276761; Issue ID: MSV-5141.	7.8	More Details
CVE-2025-20796	In imgsys, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10314745; Issue ID: MSV-5553.	7.8	More Details
CVE-2025-20797	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10315812; Issue ID: MSV-5534.	7.8	More Details
CVE-2025-20798	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10315812; Issue ID: MSV-5533.	7.8	More Details
CVE-2025-20799	In c2ps, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10274607; Issue ID: MSV-5049.	7.8	More Details
CVE-2025-20781	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182914; Issue ID: MSV-4699.	7.8	More Details
CVE-2025-20800	In mminfra, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10267349; Issue ID: MSV-5033.	7.8	More Details
CVE-2025-64699	An incorrect NULL DACL issue exists in SevenCs ORCA G2 2.0.1.35 (EC2007 Kernel v5.22). The regService process, which runs with SYSTEM privileges, applies a Security Descriptor to a device object with no explicitly configured DACL. This condition could allow an attacker to perform unauthorized raw disk operations, which could lead to system disruption (DoS) and exposure of sensitive data, and may facilitate local privilege escalation.	7.8	More Details
CVE-2025-15371	A vulnerability has been found in Tenda i24, 4G03 Pro, 4G05, 4G08, G0-8G-PoE, Nova MW5G and TEG5328F up to 65.10.15.6. Affected is an unknown function of the component Shadow File. Such manipulation with the input Fireitup leads to hard-coded credentials. An attack has to be approached locally. The exploit has been disclosed to the public and may be used.	7.8	More Details

CVE-2026-21673	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below have overflows and underflows in CIccXmlArrayType::ParseTextCountNum(). This vulnerability affects users of the iccDEV library who process ICC color profiles. This issue is fixed in version 2.3.1.1.	7.8	More Details
CVE-2025-57836	An issue was discovered in Samsung Magician 6.3.0 through 8.3.2 on Windows. The installer creates a temporary folder with weak permissions during installation, allowing a non-admin user to perform DLL hijacking and escalate privileges.	7.8	More Details
CVE-2026-21433	Emlog is an open source website building system. Versions up to and including 2.5.19 are vulnerable to server-side Out-of-Band (OOB) requests / SSRF via uploaded SVG files. An attacker can upload a crafted SVG to http[:]//emblog/admin/media[.]php which contains external resource references. When the server processes/renders the SVG (thumbnailing, preview, or sanitization), it issues an HTTP request to the attacker-controlled host. Impact: server-side SSRF/OOB leading to internal network probing and potential metadata/credential exposure. As of time of publication, no known patched versions are available.	7.7	More Details
CVE-2025-36589	Dell Unisphere for PowerMax, version(s) 9.2.4.x, contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to data and resources outside of the intended sphere of control.	7.6	More Details
CVE-2025-55065	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7.5	More Details
CVE-2021-47726	NuCom 11N Wireless Router 5.07.90 contains a privilege escalation vulnerability that allows non-privileged users to access administrative credentials through the configuration backup endpoint. Attackers can send a crafted HTTP GET request to the backup configuration page with a specific cookie to retrieve and decode the admin password in Base64 format.	7.5	More Details
CVE-2021-47740	KZTech JT3500V 4G LTE CPE 2.0.1 contains a session management vulnerability that allows attackers to reuse old session credentials without proper expiration. Attackers can exploit the weak session handling to maintain unauthorized access and potentially compromise device authentication mechanisms.	7.5	More Details
CVE-2021-47741	ZBL EPON ONU Broadband Router V100R001 contains a privilege escalation vulnerability that allows limited administrative users to elevate access by sending requests to configuration endpoints. Attackers can exploit the vulnerability by accessing the configuration backup or password page to disclose the super user password and gain additional privileged functionalities.	7.5	More Details
CVE-2021-47744	Cypress Solutions CTM-200/CTM-ONE 1.3.6 contains hard-coded credentials vulnerability in Linux distribution that exposes root access. Attackers can exploit the static 'Chameleon' password to gain remote root access via Telnet or SSH on affected devices.	7.5	More Details
CVE-2025-69342	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in VanKarWai Calafate calafate allows PHP Local File Inclusion.This issue affects Calafate: from n/a through <= 1.7.7.	7.5	More Details
CVE-2025-59379	DwyerOmega Isensix Advanced Remote Monitoring System (ARMS) 1.5.7 allows an attacker to retrieve sensitive information from the underlying SQL database via Blind SQL Injection through the user parameter in the login page. This allows an attacker to steal credentials, which may be cleartext, from existing users (and admins) and use them to authenticate to the application.	7.5	More Details
CVE-2020-	Sony BRAVIA Digital Signage 1.7.8 contains an information disclosure vulnerability that allows unauthenticated attackers to access sensitive system details through API endpoints. Attackers can retrieve network interface information, server configurations,	7.5	More Details

36922	and system metadata by sending requests to the exposed system API.		
CVE-2020-36924	Sony BRAVIA Digital Signage 1.7.8 contains a remote file inclusion vulnerability that allows attackers to inject arbitrary client-side scripts through the content material URL parameter. Attackers can exploit this vulnerability to hijack user sessions, execute cross-site scripting code, and modify display content by manipulating the input material type.	7.5	More Details
CVE-2025-9110	An exposure of sensitive system information to an unauthorized control sphere vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to read application data. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3332 build 20251128 and later QuTS hero h5.2.8.3321 build 20251117 and later QuTS hero h5.3.1.3250 build 20250912 and later	7.5	More Details
CVE-2025-67269	An integer underflow vulnerability exists in the `nextstate()` function in `gpsd/packet.c` of gpsd versions prior to commit `ffa1d6f40bca0b035fc7f5e563160ebb67199da7`. When parsing a NAVCOM packet, the payload length is calculated using `lexer->length = (size_t)c - 4` without checking if the input byte `c` is less than 4. This results in an unsigned integer underflow, setting `lexer->length` to a very large value (near `SIZE_MAX`). The parser then enters a loop attempting to consume this massive number of bytes, causing 100% CPU utilization and a Denial of Service (DoS) condition.	7.5	More Details
CVE-2020-36921	RED-V Super Digital Signage System 5.1.1 contains an information disclosure vulnerability that allows unauthenticated attackers to access sensitive webserver log files. Attackers can visit multiple endpoints to retrieve system resources and debug log information without authentication.	7.5	More Details
CVE-2020-36905	FIBARO System Home Center 5.021 contains a remote file inclusion vulnerability in the undocumented proxy API that allows attackers to include arbitrary client-side scripts. Attackers can exploit the 'url' GET parameter to inject malicious JavaScript and potentially hijack user sessions or manipulate page content.	7.5	More Details
CVE-2020-36917	iDS6 DSSPro Digital Signage System 6.2 contains a sensitive information disclosure vulnerability that allows remote attackers to intercept authentication credentials through cleartext cookie transmission. Attackers can exploit the autoSave feature to capture user passwords during man-in-the-middle attacks on HTTP communications.	7.5	More Details
CVE-2020-36914	QiHang Media Web Digital Signage 3.0.9 contains a sensitive information disclosure vulnerability that allows remote attackers to intercept user authentication credentials through cleartext cookie transmission. Attackers can perform man-in-the-middle attacks to capture and potentially misuse stored authentication credentials transmitted in an insecure manner.	7.5	More Details
CVE-2025-68272	Signal K Server is a server application that runs on a central hub in a boat. A Denial of Service (DoS) vulnerability in versions prior to 2.19.0 allows an unauthenticated attacker to crash the SignalK Server by flooding the access request endpoint (`/signalk/v1/access/requests`). This causes a "JavaScript heap out of memory" error due to unbounded in-memory storage of request objects. Version 2.19.0 fixes the issue.	7.5	More Details
CVE-2026-21428	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to version 0.30.0, the ``write_headers`` function does not check for CR & LF characters in user supplied headers, allowing untrusted header value to escape header lines. This vulnerability allows attackers to add extra headers, modify request body unexpectedly & trigger an SSRF attack. When combined with a server that supports http1.1 pipelining (springboot, python twisted etc), this can be used for server side request forgery (SSRF). Version 0.30.0 fixes this issue.	7.5	More Details
CVE-2020-	Aerohive HiveOS contains a denial of service vulnerability in the NetConfig UI that allows unauthenticated attackers to render the web interface unusable. Attackers can send a crafted HTTP request to the action.php5 script with specific parameters to	7.5	More Details

36907	trigger a 5-minute service disruption.		
CVE-2020-36915	Adtec Digital SignEdje Digital Signage Player v2.08.28 contains multiple hardcoded default credentials that allow unauthenticated remote access to web, telnet, and SSH interfaces. Attackers can exploit these credentials to gain root-level access and execute system commands across multiple Adtec Digital product versions.	7.5	More Details
CVE-2025-67158	An authentication bypass in the /cgi-bin/jvsweb.cgi endpoint of Revotech I6032W-FHW v1.0.0014 - 20210517 allows attackers to access sensitive information and escalate privileges via a crafted HTTP request.	7.5	More Details
CVE-2025-20794	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689259 / MOLY01586470; Issue ID: MSV-4847.	7.5	More Details
CVE-2025-67419	A Denial of Service (DoS) vulnerability in evershop 2.1.0 and prior allows unauthenticated attackers to exhaust the application server's resources via the "GET /images" API. The application fails to limit the height of the use-element shadow tree or the dimensions of pattern tiles during the processing of SVG files, resulting in unbounded resource consumption and system-wide denial of service.	7.5	More Details
CVE-2025-68131	cbor2 provides encoding and decoding for the Concise Binary Object Representation (CBOR) serialization format. Starting in version 3.0.0 and prior to version 5.8.0, whhen a CBORDecoder instance is reused across multiple decode operations, values marked with the shareable tag (28) persist in memory and can be accessed by subsequent CBOR messages using the sharedref tag (29). This allows an attacker-controlled message to read data from previously decoded messages if the decoder is reused across trust boundaries. Version 5.8.0 patches the issue.	7.5	More Details
CVE-2025-67159	Vatilon v1.12.37-20240124 was discovered to transmit user credentials in plaintext.	7.5	More Details
CVE-2025-67160	An issue in Vatilon v1.12.37-20240124 allows attackers to access sensitive directories and files via a directory traversal.	7.5	More Details
CVE-2025-13029	The Knowband Mobile App Builder WordPress plugin before 3.0.0 does not have authorisation when deleting users via its REST API, allowing unauthenticated attackers to delete arbitrary users.	7.5	More Details
CVE-2026-21452	MessagePack for Java is a serializer implementation for Java. A denial-of-service vulnerability exists in versions prior to 0.9.11 when deserializing .msgpack files containing EXT32 objects with attacker-controlled payload lengths. While MessagePack-Java parses extension headers lazily, it later trusts the declared EXT payload length when materializing the extension data. When ExtensionValue.getData() is invoked, the library attempts to allocate a byte array of the declared length without enforcing any upper bound. A malicious .msgpack file of only a few bytes can therefore trigger unbounded heap allocation, resulting in JVM heap exhaustion, process termination, or service unavailability. This vulnerability is triggered during model loading / deserialization, making it a model format vulnerability suitable for remote exploitation. The vulnerability enables a remote denial-of-service attack against applications that deserialize untrusted .msgpack model files using MessagePack for Java. A specially crafted but syntactically valid .msgpack file containing an EXT32 object with an attacker-controlled, excessively large payload length can trigger unbounded memory allocation during deserialization. When the model file is loaded, the library trusts the declared length metadata and attempts to allocate a byte array of that size, leading to rapid heap exhaustion, excessive garbage collection, or immediate JVM termination with an OutOfMemoryError. The attack requires no malformed bytes, user interaction,	7.5	More Details

	or elevated privileges and can be exploited remotely in real-world environments such as model registries, inference services, CI/CD pipelines, and cloud-based model hosting platforms that accept or fetch .msgpack artifacts. Because the malicious file is extremely small yet valid, it can bypass basic validation and scanning mechanisms, resulting in complete service unavailability and potential cascading failures in production systems. Version 0.9.11 fixes the vulnerability.		
CVE-2025-68033	Insertion of Sensitive Information Into Sent Data vulnerability in Brecht Custom Related Posts allows Retrieve Embedded Sensitive Data.This issue affects Custom Related Posts: from n/a through 1.8.0.	7.5	More Details
CVE-2025-68547	Missing Authorization vulnerability in WPweb Follow My Blog Post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Follow My Blog Post: from n/a through 2.4.0.	7.5	More Details
CVE-2025-68850	Missing Authorization vulnerability in Codepeople Sell Downloads allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sell Downloads: from n/a through 1.1.12.	7.5	More Details
CVE-2025-20793	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01430930; Issue ID: MSV-4836.	7.5	More Details
CVE-2025-67303	An issue in ComfyUI-Manager prior to version 3.38 allowed remote attackers to potentially manipulate its configuration and critical data. This was due to the application storing its files in an insufficiently protected location that was accessible via the web interface	7.5	More Details
CVE-2024-30516	Improper Validation of Specified Quantity in Input vulnerability in SaasProject Booking Package allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Booking Package: from n/a through 1.6.27.	7.5	More Details
CVE-2025-46255	Missing Authorization vulnerability in Marketing Fire LLC LoginWP - Pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LoginWP - Pro: from n/a through 4.0.8.5.	7.5	More Details
CVE-2025-59467	A Cross-Site Scripting (XSS) vulnerability in the UCRM Argentina AFIP invoices Plugin (v1.2.0 and earlier) could allow privilege escalation if an Administrator is tricked into visiting a crafted malicious page. This plugin is disabled by default. Affected Products: UCRM Argentina AFIP invoices Plugin (Version 1.2.0 and earlier) Mitigation: Update UCRM Argentina AFIP invoices Plugin to Version 1.3.0 or later.	7.5	More Details
CVE-2025-43706	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2400, 1580, 9110, W920, W930, Modem 5123, and Modem 5400. Incorrect handling of RRC packets leads to a Denial of Service.	7.5	More Details
CVE-2020-36904	Selea CarPlateServer 4.0.1.6 contains a remote program execution vulnerability that allows attackers to execute arbitrary Windows binaries by manipulating the NO_LIST_EXE_PATH configuration parameter. Attackers can bypass authentication through the /cps/ endpoint and modify server configuration, including changing admin passwords and executing system commands.	7.5	More Details
CVE-2026-21507	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below have an infinite loop in the IccProfile.cpp function, CalcProfileID. This issue is fixed in version 2.3.1.1.	7.5	More Details
CVE-2025-20762	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01685181; Issue ID: MSV-	7.5	More Details

	4760.		
CVE-2025-20761	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01311265; Issue ID: MSV-4655.	7.5	More Details
CVE-2025-20760	In Modem, there is a possible read of uninitialized heap data due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01676750; Issue ID: MSV-4653.	7.5	More Details
CVE-2025-69223	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a zip bomb to be used to execute a DoS against the AIOHTTP server. An attacker may be able to send a compressed request that when decompressed by AIOHTTP could exhaust the host's memory. This issue is fixed in version 3.13.3.	7.5	More Details
CVE-2025-68953	Frappe is a full-stack web application framework. Versions 14.99.5 and below and 15.0.0 through 15.80.1 include requests that are vulnerable to path traversal attacks. Arbitrary files from the server could be retrieved due to a lack of proper sanitization on some requests. This issue is fixed in versions 14.99.6 and 15.88.1. To workaround, changing the setup to use a reverse proxy is recommended.	7.5	More Details
CVE-2026-0578	A vulnerability has been found in code-projects Online Product Reservation System 1.0. Affected by this issue is some unknown functionality of the file /handgunner-administrator/delete.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-15458	A vulnerability was determined in bg5sbk MiniCMS up to 1.8. This affects an unknown function of the file /mc-admin/post-edit.php of the component Article Handler. Executing a manipulation can lead to improper 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-2025-15457	A vulnerability was found in bg5sbk MiniCMS up to 1.8. The impacted element is an unknown function of the file /minicms/mc-admin/post.php of the component Trash File Restore Handler. Performing a manipulation results in improper authentication. 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.	7.3	More Details
CVE-2025-15456	A vulnerability has been found in bg5sbk MiniCMS up to 1.8. The affected element is an unknown function of the file /mc-admin/page-edit.php of the component Publish Page Handler. Such manipulation leads to improper authentication. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The existence of this vulnerability is still disputed at present. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15447	A vulnerability has been found in Seeyon Zhiyuan OA Web Application System up to 20251223. This affects an unknown function of the file /assetsGroupReport/assetsService.j%73p. The manipulation of the argument unitCode leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-	A flaw has been found in Seeyon Zhiyuan OA Web Application System up to 20251223. The impacted element is an unknown function of the file /assetsGroupReport/fixedAssetsList.j%73p. Executing a manipulation of the argument		More

2025-15446	unitCode can lead to sql 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.	7.3	Details
CVE-2026-0579	A vulnerability was found in code-projects Online Product Reservation System 1.0. This affects an unknown part of the file /handgunner-administrator/edit.php of the component POST Parameter Handler. The manipulation of the argument prod_id/name/price/model/serial results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-0575	A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. This impacts an unknown function of the file /handgunner-administrator/adminlogin.php of the component Administrator Login. Such manipulation of the argument emailadd/pass leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-0576	A vulnerability was detected in code-projects Online Product Reservation System 1.0. Affected is an unknown function of the file /handgunner-administrator/prod.php of the component Parameter Handler. Performing manipulation of the argument cat/price/name/model/serial results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-0585	A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. Impacted is an unknown function of the file /order_view.php of the component GET Parameter Handler. Such manipulation of the argument transaction_id leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-3653	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains an improper access control vulnerability that allows unauthorized device manipulation by accepting arbitrary serial numbers without ownership verification. Attackers can control any device by sending serial numbers to device control APIs to change feeding schedules, trigger manual feeds, access camera feeds, and modify device settings without authorization checks.	7.3	More Details
CVE-2025-3646	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains an authorization bypass vulnerability that allows unauthorized users to add users as shared owners to any device by exploiting missing permission checks. Attackers can send requests to the device share API to gain unauthorized access to devices and view owner information without proper authorization validation.	7.3	More Details
CVE-2025-15364	The Download Manager plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.3.40. This is due to the plugin not properly validating a user's identity prior to updating their details like password. This makes it possible for unauthenticated attackers to change user's passwords, except administrators, and leverage that to gain access to their account.	7.3	More Details
CVE-2026-0570	A vulnerability was found in code-projects Online Music Site 1.0. This impacts an unknown function of the file /Frontend/Feedback.php. Performing manipulation of the argument fname results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-0569	A vulnerability has been found in code-projects Online Music Site 1.0. This affects an unknown function of the file /Frontend/AlbumByCategory.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-2026-0568	A flaw has been found in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Frontend/ViewSongs.php. This manipulation of the argument ID 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-2026-0567	A vulnerability was detected in code-projects Content Management System 1.0. The affected element is an unknown function of the file /pages.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-0583	A security flaw has been discovered in code-projects Online Product Reservation System 1.0. This vulnerability affects unknown code of the file app/user/login.php of the component User Login. The manipulation of the argument emailadd 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-2025-15408	A vulnerability was found in code-projects Online Guitar Store 1.0. Affected is an unknown function of the file /admin/Create_product.php. Performing manipulation of the argument dre_title results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-0605	A security vulnerability has been detected in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. Such manipulation of the argument username/password leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-0607	A flaw has been found in code-projects Online Music Site 1.0. This affects an unknown part of the file /Administrator/PHP/AdminViewSongs.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-15434	A vulnerability was detected in Yonyou KSOA 9.0. Affected is an unknown function of the file /kp/PrintZPYG.jsp. The manipulation of the argument zpjhid results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15435	A flaw has been found in Yonyou KSOA 9.0. Affected by this vulnerability is an unknown functionality of the file /worksheet/work_update.jsp. This manipulation of the argument Report causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15427	A security flaw has been discovered in Seeyon Zhiyuan OA Web Application System up to 20251222. This impacts an unknown function of the file /carManager/carUseDetailList.j%73p. The manipulation of the argument CAR_BRAND_NO results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15426	A vulnerability was identified in jackying H-ui.admin up to 3.1. This affects an unknown function in the library /lib/webuploader/0.1.5/server/preview.php. The manipulation leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15425	A vulnerability was determined in Yonyou KSOA 9.0. The impacted element is an unknown function of the file /worksheet/del_user.jsp of the component HTTP GET Parameter Handler. Executing manipulation of the argument ID can lead to sql injection. The attack can be executed 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
	A vulnerability was found in Yonyou KSOA 9.0. The affected element is an unknown		

CVE-2025-15424	function of the file /worksheet/agent_worksdel.jsp of the component HTTP GET Parameter Handler. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15421	A vulnerability was detected in Yonyou KSOA 9.0. This vulnerability affects unknown code of the file /worksheet/agent_worksadd.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15420	A security vulnerability has been detected in Yonyou KSOA 9.0. This affects an unknown part of the file /worksheet/agent_work_report.jsp. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-15436	A vulnerability has been found in Yonyou KSOA 9.0. Affected by this issue is some unknown functionality of the file /worksheet/work_edit.jsp. Such manipulation of the argument Report 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.	7.3	More Details
CVE-2025-15410	A vulnerability was identified in code-projects Online Guitar Store 1.0. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument L_email leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-15409	A vulnerability was determined in code-projects Online Guitar Store 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/Delete_product.php. Executing manipulation of the argument del_pro can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-0546	A vulnerability was determined in code-projects Content Management System 1.0. This impacts an unknown function of the file search.php. This manipulation of the argument Value causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-0565	A weakness has been identified in code-projects Content Management System 1.0. This issue affects some unknown processing of the file /admin/delete.php. Executing manipulation of the argument del can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2025-15407	A vulnerability has been found in code-projects Online Guitar Store 1.0. This impacts an unknown function of the file /admin/Create_category.php. Such manipulation of the argument dre_Ctitle leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-0592	A security flaw has been discovered in code-projects Online Product Reservation System 1.0. This affects an unknown function of the file /handgunner-administrator/register_code.php of the component User Registration Handler. Performing a manipulation of the argument fname/lname/address/city/province/country/zip/tel_no/email/username results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-	A security flaw has been discovered in itsourcecode School Management System 1.0. This affects an unknown part of the file /student/index.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The	7.3	More Details

0544	exploit has been released to the public and may be used for attacks.		
CVE-2026-0589	A vulnerability was found in code-projects Online Product Reservation System 1.0. Impacted is an unknown function of the component Administration Backend. The manipulation results in improper authentication. The attack may be performed from remote. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-0606	A vulnerability was detected in code-projects Online Music Site 1.0. Affected by this issue is some unknown functionality of the file /FrontEnd/Albums.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-66376	Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13 allows Classic UI stored XSS via Cascading Style Sheets (CSS) @import directives in an HTML e-mail message.	7.2	More Details
CVE-2025-14997	The BuddyPress Xprofile Custom Field Types plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'delete_field' function in all versions up to, and including, 1.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	7.2	More Details
CVE-2025-5965	In the backup parameters, a user with high privilege is able to concatenate custom instructions to the backup setup. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Centreon Infra Monitoring (Backup configuration in the administration setup modules) allows OS Command Injection.This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19.	7.2	More Details
CVE-2025-66648	vega-functions provides function implementations for the Vega expression language. Prior to version 6.1.1, for sites that allow users to supply untrusted user input, malicious use of an internal function (not part of the public API) could be used to run unintentional javascript (XSS). This issue is fixed in vega-functions `6.1.1`. There is no workaround besides upgrading. Using `vega.expressionInterpreter` as described in CSP safe mode does not prevent this issue.	7.2	More Details
CVE-2025-68619	Signal K Server is a server application that runs on a central hub in a boat. Versions prior to 2.19.0 of the appstore interface allow administrators to install npm packages through a REST API endpoint. While the endpoint validates that the package name exists in the npm registry as a known plugin or webapp, the version parameter accepts arbitrary npm version specifiers including URLs. npm supports installing packages from git repositories, GitHub shorthand syntax, and HTTP/HTTPS URLs pointing to tarballs. When npm installs a package, it can automatically execute any `postinstall` script defined in `package.json`, enabling arbitrary code execution. The vulnerability exists because npm's version specifier syntax is extremely flexible, and the SignalK code passes the version parameter directly to npm without sanitization. An attacker with admin access can install a package from an attacker-controlled source containing a malicious `postinstall` script. Version 2.19.0 contains a patch for the issue.	7.2	More Details
CVE-2025-23707	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matamko En Masse allows Reflected XSS.This issue affects En Masse: from n/a through 1.0.	7.1	More Details
CVE-2023-49186	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in KlbTheme Machic Core allows DOM-Based XSS.This issue affects Machic Core: from n/a through 1.2.6.	7.1	More Details
CVE-2025-49343	Cross-Site Request Forgery (CSRF) vulnerability in Socialprofilr Social Profilr allows Stored XSS.This issue affects Social Profilr: from n/a through 1.0.	7.1	More Details

CVE-2025-49345	Cross-Site Request Forgery (CSRF) vulnerability in mg12 WP-EasyArchives allows Stored XSS.This issue affects WP-EasyArchives: from n/a through 3.1.2.	7.1	More Details
CVE-2025-49353	Cross-Site Request Forgery (CSRF) vulnerability in Marcin Kijak Noindex by Path allows Stored XSS.This issue affects Noindex by Path: from n/a through 1.0.	7.1	More Details
CVE-2025-49354	Cross-Site Request Forgery (CSRF) vulnerability in Mindstien Technologies Recent Posts From Each Category allows Stored XSS.This issue affects Recent Posts From Each Category: from n/a through 1.4.	7.1	More Details
CVE-2025-68885	Cross-Site Request Forgery (CSRF) vulnerability in Page Carbajal Custom Post Status allows Stored XSS.This issue affects Custom Post Status: from n/a through 1.1.0.	7.1	More Details
CVE-2025-23667	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Christopher Churchill allows Reflected XSS.This issue affects custom-post-edit: from n/a through 1.0.4.	7.1	More Details
CVE-2025-23705	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry Zielke Zielke Design Project Gallery allows Reflected XSS.This issue affects Zielke Design Project Gallery: from n/a through 2.5.0.	7.1	More Details
CVE-2025-53235	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in osuthorpe Easy Social allows Reflected XSS.This issue affects Easy Social: from n/a through 1.3.	7.1	More Details
CVE-2025-23719	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zckevin ZhinaTwitterWidget allows Reflected XSS.This issue affects ZhinaTwitterWidget: from n/a through 1.0.	7.1	More Details
CVE-2025-23757	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proloy Chakroborty ZD Scribd iPaper allows Reflected XSS.This issue affects ZD Scribd iPaper: from n/a through 1.0.	7.1	More Details
CVE-2025-61781	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to version 6.8.1, the GraphQL mutation "WorkspacePopoverDeletionMutation" allows users to delete workspace-related objects such as dashboards and investigation cases. However, the mutation lacks proper authorization checks to verify ownership of the targeted resources. An attacker can exploit this by supplying an active UUID of another user. Since the API does not validate whether the requester owns the resource, the mutation executes successfully, resulting in unauthorized deletion of the entire workspace. Version 6.8.1 fixes the issue.	7.1	More Details
CVE-2025-30631	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team Woocommerce Sales Funnel Builder, AA-Team Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer) allows Reflected XSS.This issue affects Woocommerce Sales Funnel Builder: from n/a through 1.1; Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer): from n/a through 1.2.	7.1	More Details
CVE-2025-31054	Cross-Site Request Forgery (CSRF) vulnerability in Themefy Bloggie allows Reflected XSS.This issue affects Bloggie: from n/a through 2.0.8.	7.1	More Details
CVE-2025-47566	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomSounds allows Reflected XSS.This issue affects ZoomSounds: from n/a through 6.91.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		

2025- 50053	vulnerability in nebelhorn Blappsta Mobile App Plugin & Your native, mobile iPhone App and Android App allows Reflected XSS.This issue affects Blappsta Mobile App Plugin &#8211; Your native, mobile iPhone App and Android App: from n/a through 0.8.8.8.	7.1	More Details
CVE- 2025- 52519	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, and 2500. Improper validation of user-space input in the issimian device driver leads to information disclosure and a denial of service.	7.1	More Details
CVE- 2025- 49344	Cross-Site Request Forgery (CSRF) vulnerability in Rene Ade SensitiveTagCloud allows Stored XSS.This issue affects SensitiveTagCloud: from n/a through 1.4.1.	7.1	More Details
CVE- 2025- 49342	Cross-Site Request Forgery (CSRF) vulnerability in Wolfgang Häfelinger Custom Style allows Stored XSS.This issue affects Custom Style: from n/a through 1.0.	7.1	More Details
CVE- 2025- 59137	Cross-Site Request Forgery (CSRF) vulnerability in eLEOPARD Behance Portfolio Manager allows Stored XSS.This issue affects Behance Portfolio Manager: from n/a through 1.7.5.	7.1	More Details
CVE- 2025- 69415	In Plex Media Server (PMS) through 1.42.2.10156, ability to access /myplex/account with a device token is not properly aligned with whether the device is currently associated with an account.	7.1	More Details
CVE- 2024- 30461	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tumult Inc Tumult Hype Animations allows DOM-Based XSS.This issue affects Tumult Hype Animations: from n/a through 1.9.11.	7.1	More Details
CVE- 2025- 69085	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins JobBank allows Reflected XSS.This issue affects JobBank: from n/a through 1.2.2.	7.1	More Details
CVE- 2025- 23608	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Omar Mohamed Mohamoud LIVE TV allows Reflected XSS.This issue affects LIVE TV: from n/a through 1.2.	7.1	More Details
CVE- 2025- 69084	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3 themes Photo Gallery allows Reflected XSS.This issue affects Photo Gallery: from n/a through 2.7.7.26.	7.1	More Details
CVE- 2024- 53735	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Corourke iPhone Webclip Manager allows Stored XSS.This issue affects iPhone Webclip Manager: from n/a through 0.5.	7.1	More Details
CVE- 2024- 30547	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Shazdeh Header Image Slider header-image-slider allows DOM-Based XSS.This issue affects Header Image Slider: from n/a through 0.3.	7.1	More Details
CVE- 2025- 49346	Cross-Site Request Forgery (CSRF) vulnerability in Peter Sterling Simple Archive Generator allows Stored XSS.This issue affects Simple Archive Generator: from n/a through 5.2.	7.1	More Details
CVE- 2025- 52739	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Sala allows Reflected XSS.This issue affects Sala: from n/a through 1.1.3.	7.1	More Details
CVE- 2025- 49028	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Mail Zoho ZeptoMail allows Stored XSS.This issue affects Zoho ZeptoMail: from n/a through 3.3.1.	7.1	More Details
	Bagisto is an open source laravel eCommerce platform. Prior to version 2.3.10, an		

CVE-2026-21447	Insecure Direct Object Reference vulnerability in the customer order reorder function allows any authenticated customer to add items from another customer's order to their own shopping cart by manipulating the order ID parameter. This exposes sensitive purchase information and enables potential fraud. Version 2.3.10 patches the issue.	7.1	More Details
CVE-2025-61037	A local privilege escalation vulnerability exists in SevenCs ORCA G2 2.0.1.35 (EC2007 Kernel v5.22). The flaw is a Time-of-Check Time-of-Use (TOCTOU) race condition in the license management logic. The regService process, which runs with SYSTEM privileges, creates a fixed directory and writes files without verifying whether the path is an NTFS reparse point. By exploiting this race condition, an attacker can replace the target directory with a junction pointing to a user-controlled path. This causes the SYSTEM-level process to drop binaries in a location fully controlled by the attacker, allowing arbitrary code execution with SYSTEM privileges. The vulnerability can be exploited by any standard user with only a single UAC confirmation, making it highly practical and dangerous in real-world environments.	7.0	More Details
CVE-2025-20779	In display, there is a possible use after free due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184084; Issue ID: MSV-4720.	7.0	More Details
CVE-2025-20801	In seninf, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10251210; Issue ID: MSV-4926.	7.0	More Details
CVE-2025-12513	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Hosts configuration form modules) allows Stored XSS to users with high privileges. This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19.	6.8	More Details
CVE-2025-13056	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Administration ACL menu configuration modules) allows Stored XSS to users with high privileges. This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19.	6.8	More Details
CVE-2025-12511	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (DSM extenstio configuration modules) allows Stored XSS to user with elevated privileges. This issue affects Infra Monitoring: from 25.10.0 before 25.10.1, from 24.10.0 before 24.10.4, from 24.04.0 before 24.04.8.	6.8	More Details
CVE-2025-20785	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149882; Issue ID: MSV-4677.	6.7	More Details
CVE-2025-20784	In display, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4683.	6.7	More Details
CVE-2025-20783	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4684.	6.7	More Details
CVE-2025-20782	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4685.	6.7	More Details

CVE-2025-20787	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149879; Issue ID: MSV-4658.	6.7	More Details
CVE-2025-20786	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149882; Issue ID: MSV-4673.	6.7	More Details
CVE-2025-20803	In dpe, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10199779; Issue ID: MSV-4504.	6.7	More Details
CVE-2025-20805	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114696; Issue ID: MSV-4480.	6.7	More Details
CVE-2025-20806	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114835; Issue ID: MSV-4479.	6.7	More Details
CVE-2025-20807	In dpe, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114841; Issue ID: MSV-4451.	6.7	More Details
CVE-2025-20804	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10198951; Issue ID: MSV-4503.	6.7	More Details
CVE-2026-21493	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below are vulnerable to Type Confusion in its CIccSingleSampledeCurveXml class during XML Curve Serialization. This issue is fixed in version 2.3.1.2.	6.6	More Details
CVE-2025-62991	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Minamaze allows Stored XSS.This issue affects Minamaze: from n/a through 1.10.1.	6.5	More Details
CVE-2025-67427	A Blind Server-Side Request Forgery (SSRF) vulnerability in evershop 2.1.0 and prior allows unauthenticated attackers to force the server to initiate an HTTP request via the "GET /images" API. The vulnerability occurs due to insufficient validation of the "src" query parameter, which permits arbitrary HTTP or HTTPS URIs, resulting in unexpected requests against internal and external networks.	6.5	More Details
CVE-2025-63000	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP for church Sermon Manager allows Stored XSS.This issue affects Sermon Manager: from n/a through 2.30.0.	6.5	More Details
CVE-2025-63005	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas WordPress Tooltips allows Stored XSS.This issue affects WordPress Tooltips: from n/a through 10.7.9.	6.5	More Details
CVE-2025-63032	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Consulting allows Stored XSS.This issue affects Consulting: from n/a through 1.5.0.	6.5	More Details

CVE-2025-39497	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dokan Dokan Pro allows Stored XSS.This issue affects Dokan Pro: from n/a through 3.14.5.	6.5	More Details
CVE-2025-39561	Missing Authorization vulnerability in Marketing Fire, LLC LoginWP - Pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LoginWP - Pro: from n/a through 4.0.8.5.	6.5	More Details
CVE-2025-62756	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ivaudore The Moneytizer allows DOM-Based XSS.This issue affects The Moneytizer: from n/a through 10.0.6.	6.5	More Details
CVE-2025-62757	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebMan Design | Oliver Juhas WebMan Amplifier allows DOM-Based XSS.This issue affects WebMan Amplifier: from n/a through 1.5.12.	6.5	More Details
CVE-2025-49358	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ruhul Amin Content Fetcher allows DOM-Based XSS.This issue affects Content Fetcher: from n/a through 1.1.	6.5	More Details
CVE-2025-62135	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in landwire Responsive Block Control allows DOM-Based XSS.This issue affects Responsive Block Control: from n/a through 1.2.9.	6.5	More Details
CVE-2025-62748	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Genetech Products Web and WooCommerce Addons for WPBakery Builder allows DOM-Based XSS.This issue affects Web and WooCommerce Addons for WPBakery Builder: from n/a through 1.5.	6.5	More Details
CVE-2025-62749	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bainternet User Specific Content allows DOM-Based XSS.This issue affects User Specific Content: from n/a through 1.0.6.	6.5	More Details
CVE-2025-62111	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webvitaly Extra Shortcodes allows Stored XSS.This issue affects Extra Shortcodes: from n/a through 2.2.	6.5	More Details
CVE-2025-62752	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kalender.Digital Calendar.Online / Kalender.Digital allows DOM-Based XSS.This issue affects Calendar.Online / Kalender.Digital: from n/a through 1.0.11.	6.5	More Details
CVE-2026-21634	A malicious actor with access to the adjacent network could overflow the UniFi Protect Application (Version 6.1.79 and earlier) discovery protocol causing it to restart. Affected Products: UniFi Protect Application (Version 6.1.79 and earlier). Mitigation: Update your UniFi Protect Application to Version 6.2.72 or later.	6.5	More Details
CVE-2025-49357	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Audiomack allows Stored XSS.This issue affects Audiomack: from n/a through 1.4.8.	6.5	More Details
CVE-2020-36909	SnapGear Management Console SG560 3.1.5 contains a file manipulation vulnerability that allows authenticated users to read, write, and delete files using the edit_config_files CGI script. Attackers can manipulate POST request parameters in /cgi-bin/cgix/edit_config_files to access and modify files outside the intended /etc/config/ directory.	6.5	More Details
CVE-2025-62118	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kcseopro AdWords Conversion Tracking Code allows Stored XSS.This issue affects AdWords Conversion Tracking Code: from n/a through 1.0.	6.5	More Details
CVE-	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then		

2025-53592	exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	6.5	More Details
CVE-2025-9637	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability and status checks on multiple functions in all versions up to, and including, 10.3.1. This makes it possible for unauthenticated attackers to view the details of unpublished, private, or password-protected quizzes, as well as submit file responses to questions from those quizzes, which allow file upload.	6.5	More Details
CVE-2025-5919	The Appointment Booking and Scheduling Calendar Plugin – WP Timetics plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the update and register_routes functions in all versions up to, and including, 1.0.36. This makes it possible for unauthenticated attackers to view and modify booking details.	6.5	More Details
CVE-2025-62852	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: QTS 5.2.8.3332 build 20251128 and later	6.5	More Details
CVE-2026-0604	The FastDup – Fastest WordPress Migration & Duplicator plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.7 via the 'dir_path' parameter in the 'njt-fastdup/v1/template/directory-tree' REST API endpoint. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary directories on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-53597	A buffer overflow vulnerability has been reported to affect License Center. If a remote attacker gains an administrator account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: License Center 2.0.36 and later	6.5	More Details
CVE-2025-14153	The Page Expire Popup/Redirection for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' shortcode attribute in all versions up to, and including, 1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-52871	An out-of-bounds read vulnerability has been reported to affect License Center. If a remote attacker gains a user account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following version: License Center 2.0.36 and later	6.5	More Details
CVE-2025-48721	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: QTS 5.2.8.3332 build 20251128 and later	6.5	More Details
CVE-2025-13652	The CBX Bookmark & Favorite plugin for WordPress is vulnerable to generic SQL Injection via the ‘orderby’ parameter in all versions up to, and including, 2.0.4 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
	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin		

CVE-2025-11723	plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.6.9.5 via the hash() function due to use of a hardcoded fall-back salt. This makes it possible for unauthenticated attackers to generate a valid token across sites running the plugin that have not manually set a salt in the wp-config.php file and access booking information that will allow them to make modifications.	6.5	More Details
CVE-2025-63020	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wayne Allen Postie postie allows Stored XSS.This issue affects Postie: from n/a through 1.9.73.	6.5	More Details
CVE-2025-53593	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	6.5	More Details
CVE-2025-53591	A use of externally-controlled format string vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to obtain secret data or modify memory. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	6.5	More Details
CVE-2025-62125	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Anshul Gangrade Custom Background Changer custom-background-changer allows Stored XSS.This issue affects Custom Background Changer: from n/a through 3.0.	6.5	More Details
CVE-2025-47208	An allocation of resources without limits or throttling vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following versions: QTS 5.2.6.3195 build 20250715 and later QuTS hero h5.2.6.3195 build 20250715 and later	6.5	More Details
CVE-2025-44013	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.6.3195 build 20250715 and later QuTS hero h5.2.6.3195 build 20250715 and later	6.5	More Details
CVE-2025-65328	Mega-Fence (webgate-lib.*) 25.1.914 and prior trusts the first value of the X-Forwarded-For (XFF) header as the client IP without validating a trusted proxy chain. An attacker can supply an arbitrary XFF value in a remote request to spoof the client IP, which is then propagated to security-relevant state (e.g., WG_CLIENT_IP cookie). Deployments that rely on this value for IP allowlists may be bypassed.	6.5	More Details
CVE-2025-62097	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SEOthemes SEO Slider allows DOM-Based XSS.This issue affects SEO Slider: from n/a through 1.1.1.	6.5	More Details
CVE-2025-62096	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Maximum Products per User for WooCommerce allows Stored XSS.This issue affects Maximum Products per User for WooCommerce: from n/a through 4.4.2.	6.5	More Details
CVE-2025-62095	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Neilgee Bootstrap Modals allows Stored XSS.This issue affects Bootstrap Modals: from n/a through 1.3.2.	6.5	More Details

CVE-2025-12685	The WPBookit WordPress plugin through 1.0.7 lacks a CSRF check when deleting customers. This could allow an unauthenticated attacker to delete any customer through a CSRF attack.	6.5	More Details
CVE-2025-69197	Pterodactyl is a free, open-source game server management panel. Versions 1.11.11 and below allow TOTP to be used multiple times during its validity window. Users with 2FA enabled are prompted to enter a token during sign-in, and afterward it is not sufficiently marked as used in the system. This allows an attacker who intercepts that token to use it in addition to a known username/password during the 60-second token validity window. The attacker must have intercepted a valid 2FA token (for example, during a screen share). This issue is fixed in version 1.12.0.	6.5	More Details
CVE-2025-62990	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Beaver Builder addons-for-beaver-builder allows Stored XSS.This issue affects Livemesh Addons for Beaver Builder: from n/a through 3.9.2.	6.5	More Details
CVE-2025-62744	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Steman Page Title Splitter allows Stored XSS.This issue affects Page Title Splitter: from n/a through 2.5.9.	6.5	More Details
CVE-2025-62743	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zookatron MyBookTable Bookstore allows Stored XSS.This issue affects MyBookTable Bookstore: from n/a through 3.5.5.	6.5	More Details
CVE-2025-62742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Curator.Io allows Stored XSS.This issue affects Curator.Io: from n/a through 1.9.5.	6.5	More Details
CVE-2025-48768	Release of Invalid Pointer or Reference vulnerability was discovered in fs/inode/fs_inoderemove code of the Apache NuttX RTOS that allowed root filesystem inode removal leading to a debug assert trigger (that is disabled by default), NULL pointer dereference (handled differently depending on the target architecture), or in general, a Denial of Service. This issue affects Apache NuttX RTOS: from 10.0.0 before 12.10.0. Users of filesystem based services with write access that were exposed over the network (i.e. FTP) are affected and recommended to upgrade to version 12.10.0 that fixes the issue.	6.5	More Details
CVE-2025-9318	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to time-based SQL Injection via the ‘is_linking’ parameter in all versions up to, and including, 10.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-15235	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has a Missing Authorization vulnerability, allowing authenticated remote attackers to modify specific network packet parameters, enabling certain system functions to access other users' files.	6.5	More Details
CVE-2025-62137	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shuttlethemes Shuttle allows Stored XSS.This issue affects Shuttle: from n/a through 1.5.0.	6.5	More Details
CVE-2025-15238	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-	A flaw has been found in bg5sbk MiniCMS up to 1.8. Impacted is the function delete_page of the file /minicms/mc-admin/page.php of the component File Recovery Request Handler. This manipulation causes improper authentication. The attack is	6.5	More

15455	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.		Details
CVE-2025-15239	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-69357	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) thegem-elements-elementor allows Stored XSS.This issue affects TheGem Theme Elements (for Elementor): from n/a through <= 5.11.0.	6.5	More Details
CVE-2025-28973	Path Traversal: '.../...//' vulnerability in AA-Team Pro Bulk Watermark Plugin for WordPress allows Path Traversal.This issue affects Pro Bulk Watermark Plugin for WordPress: from n/a through 2.0.	6.5	More Details
CVE-2025-69334	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Wishlist for WooCommerce wish-list-for-woocommerce allows Stored XSS.This issue affects Wishlist for WooCommerce: from n/a through <= 3.3.0.	6.5	More Details
CVE-2025-69350	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Accordion accordions-wp allows Stored XSS.This issue affects Accordion: from n/a through <= 3.0.3.	6.5	More Details
CVE-2025-3660	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains a broken access control vulnerability that allows authenticated users to access other users' pet data by exploiting missing ownership verification. Attackers can send requests to /member/pet/detailV2 with arbitrary pet IDs to retrieve sensitive information including pet details, member IDs, and avatar URLs without proper authorization checks.	6.5	More Details
CVE-2025-69351	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shahjahan Jewel Ninja Tables ninja-tables allows Blind SQL Injection.This issue affects Ninja Tables: from n/a through <= 5.2.4.	6.5	More Details
CVE-2025-68014	Insertion of Sensitive Information Into Sent Data vulnerability in Awethemes AweBooking allows Retrieve Embedded Sensitive Data.This issue affects AweBooking: from n/a through 3.2.26.	6.5	More Details
CVE-2025-15115	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains an authentication bypass vulnerability that allows unauthenticated attackers to access any user account by exploiting OAuth token validation flaws in the social login system. Attackers can send requests to /member/auth/thirdLogin with arbitrary Google IDs and phoneBrand parameters to obtain full session tokens and account access without proper OAuth verification.	6.5	More Details
CVE-2024-31088	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPShop.Ru AdsPlace'r – Ad Manager, Inserter, AdSense Ads allows DOM-Based XSS.This issue affects AdsPlace'r – Ad Manager, Inserter, AdSense Ads: from n/a through 1.1.5.	6.5	More Details
CVE-2025-63021	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codetipi Valenti Engine allows DOM-Based XSS.This issue affects Valenti Engine: from n/a through 1.0.3.	6.5	More Details
CVE-2025-62136	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Melos allows Stored XSS.This issue affects Melos: from n/a through 1.6.0.	6.5	More Details
CVE-2025-69362	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POSIMYTH UiChemy uichemy allows Stored XSS.This issue affects UiChemy: from n/a through <= 4.4.2.	6.5	More Details

CVE-2025-69360	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for WPBakery) thegem-elements allows DOM-Based XSS.This issue affects TheGem Theme Elements (for WPBakery): from n/a through <= 5.11.0.	6.5	More Details
CVE-2025-62146	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maksym Marko MX Time Zone Clocks allows Stored XSS.This issue affects MX Time Zone Clocks: from n/a through 5.1.1.	6.5	More Details
CVE-2025-62758	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Funnelforms Funnelforms Free allows DOM-Based XSS.This issue affects Funnelforms Free: from n/a through 3.8.	6.5	More Details
CVE-2025-62759	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Tadlock Series allows Stored XSS.This issue affects Series: from n/a through 2.0.1.	6.5	More Details
CVE-2025-62760	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev BuddyPress Activity Shortcode allows Stored XSS.This issue affects BuddyPress Activity Shortcode: from n/a through 1.1.8.	6.5	More Details
CVE-2023-51513	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in INTINITUM FORM Geo Controller allows DOM-Based XSS.This issue affects Geo Controller: from n/a through 8.5.2.	6.5	More Details
CVE-2024-23511	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows DOM-Based XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.3.3.	6.5	More Details
CVE-2025-68280	Improper Restriction of XML External Entity Reference vulnerability in Apache SIS. It is possible to write XML files in such a way that, when parsed by Apache SIS, an XML file reveals to the attacker the content of a local file on the server running Apache SIS. This vulnerability impacts the following SIS services: * Reading of GeoTIFF files having the GEO_METADATA tag defined by the Defense Geospatial Information Working Group (DGIWG). * Parsing of ISO 19115 metadata in XML format. * Parsing of Coordinate Reference Systems defined in the GML format. * Parsing of files in GPS Exchange Format (GPX). This issue affects Apache SIS from versions 0.4 through 1.5 inclusive. Users are recommended to upgrade to version 1.6, which will fix the issue. In the meantime, the security vulnerability can be avoided by launching Java with the javax.xml.accessExternalDTD system property sets to a comma-separated list of authorized protocols. For example: java -Djavax.xml.accessExternalDTD="" ...	6.5	More Details
CVE-2025-62761	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BasePress Knowledge Base documentation & wiki plugin – BasePress allows Stored XSS.This issue affects Knowledge Base documentation & wiki plugin – BasePress: from n/a through 2.17.0.1.	6.5	More Details
CVE-2025-62992	Cross-Site Request Forgery (CSRF) vulnerability in Everest themes Everest Backup allows Path Traversal.This issue affects Everest Backup: from n/a through 2.3.9.	6.5	More Details
CVE-2025-46696	Dell Secure Connect Gateway (SCG) 5.0 Appliance and Application, version(s) versions 5.26 to 5.30, contain(s) an Execution with Unnecessary Privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	6.4	More Details
CVE-2025-14120	The URL Image Importer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.7 due to insufficient sanitization of SVG files. 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.	6.4	More Details

CVE-2025-14438	The Xagio SEO – AI Powered SEO plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.1.0.30 via the 'pixabayDownloadImage' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.4	More Details
CVE-2025-4776	The Phlox theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` HTML attribute in all versions up to, and including, 2.17.7 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-2025-12067	The Table Field Add-on for ACF and SCF plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table Cell Content in all versions up to, and including, 1.3.30 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-2025-13746	The ForumWP – Forum & Discussion Board plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User's Display Name in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14627	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.35. This is due to inadequate validation of the resolved URL after following Bitly shortlink redirects in the `upload_function()` method. While the initial URL is validated using `wp_http_validate_url()`, when a Bitly shortlink is detected, the `unshorten_bitly_url()` function follows redirects to the final destination URL without re-validating it. This makes it possible for authenticated attackers with Contributor-level access or higher to make the server perform HTTP requests to arbitrary internal endpoints, including localhost, private IP ranges, and cloud metadata services (e.g., 169.254.169.254), potentially exposing sensitive internal data.	6.4	More Details
CVE-2025-14552	The MediaPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's mpp-uploader shortcode in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0581	A vulnerability was determined in Tenda AC1206 15.03.06.23. Affected by this issue is the function formBehaviorManager of the file /goform/BehaviorManager of the component httpd. Executing a manipulation of the argument modulename/option/data/switch can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-	Signal K Server is a server application that runs on a central hub in a boat. Versions prior to 2.19.0 of the access request system have two related features that when combined by themselves and with an information disclosure vulnerability enable convincing social engineering attacks against administrators. When a device creates an access request, it specifies three fields: `clientId`, `description`, and `permissions`. The SignalK admin UI displays the `description` field prominently to the administrator when showing pending requests, but the actual `permissions` field (which determines the access level granted) is less visible or displayed separately. This allows an attacker to request `admin` permissions while providing a description that suggests readonly access. The access request handler trusts the `X-Forwarded-For` HTTP header without validation to determine the client's IP address. This header is intended to preserve the	6.3	More Details

69203	original client IP when requests pass through reverse proxies, but when trusted unconditionally, it allows attackers to spoof their IP address. The spoofed IP is displayed to administrators in the access request approval interface, potentially making malicious requests appear to originate from trusted internal network addresses. Since device/source names can be enumerated via the information disclosure vulnerability, an attacker can impersonate a legitimate device or source, craft a convincing description, spoof a trusted internal IP address, and request elevated permissions, creating a highly convincing social engineering scenario that increases the likelihood of administrator approval. Users should upgrade to version 2.19.0 to fix this issue.		
CVE-2025-15450	A vulnerability was identified in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. Affected by this vulnerability is the function findOrderHosNum of the file /ssm_pro/orderHos/. Such manipulation of the argument hospitalAddress/hospitalName leads to sql injection. 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.	6.3	More Details
CVE-2025-15448	A vulnerability was found in cld378632668 JavaMall up to 994f1e2b019378ec9444cdf3fce2d5b5f72d28f0. This impacts the function Upload of the file src/main/java/com/macro/mall/controller/MinioController.java. The manipulation results in unrestricted upload. It is possible to launch the attack remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-0577	A flaw has been found in code-projects Online Product Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /handgunner-administrator/prod.php. Executing manipulation can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-0574	A weakness has been identified in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This affects the function saveUserRole of the file warehouse\src\main\java\com\yeqifu\sys\controller\UserController.java of the component Request Handler. This manipulation causes improper authorization. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified.	6.3	More Details
CVE-2026-0582	A vulnerability was identified in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/edit_activity_query.php. The manipulation of the argument Title leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-0584	A weakness has been identified in code-projects Online Product Reservation System 1.0. This issue affects some unknown processing of the file app/products/left_cart.php. This manipulation of the argument ID 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.	6.3	More Details
CVE-2025-15393	A security vulnerability has been detected in Kohana KodiCMS up to 13.82.135. This impacts the function Save of the file cms/modules/kodicms/classes/kodicms/model/file.php of the component Layout API Endpoint. The manipulation of the argument content leads to code injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2025-68029	Insertion of Sensitive Information Into Sent Data vulnerability in WP Swings Wallet System for WooCommerce allows Retrieve Embedded Sensitive Data.This issue affects Wallet System for WooCommerce: from n/a through 2.7.2.	6.3	More Details
CVE-2025-15375	A flaw has been found in EyouCMS up to 1.7.7. The impacted element is the function unserialize of the file application/api/controller/Ajax.php of the component arcpagelist Handler. Executing manipulation of the argument attstr can lead to deserialization. The attack can be launched remotely. The exploit has been published and may be used. The vendor is "[a]cknowledging the existence of the vulnerability, we have completed the fix and will release a new version, v1.7.8".	6.3	More Details
CVE-2025-15423	A vulnerability has been found in EmpireSoft EmpireCMS up to 8.0. Impacted is the function CheckSaveTranFiletype of the file e/class/connect.php. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-0590	A vulnerability was determined in code-projects Online Product Reservation System 1.0. The affected element is an unknown function of the file /app/checkout/delete.php of the component POST Parameter Handler. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-0591	A vulnerability was identified in code-projects Online Product Reservation System 1.0. The impacted element is an unknown function of the file /app/checkout/update.php of the component Cart Update Handler. Such manipulation of the argument id/qty leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-15392	A weakness has been identified in Kohana KodiCMS up to 13.82.135. This affects the function like of the file cms/modules/pages/classes/kodicms/model/page.php of the component Search API Endpoint. Executing manipulation of the argument keyword can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-15404	A security vulnerability has been detected in campcodes School File Management System 1.0. The affected element is an unknown function of the file /save_file.php. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-0597	A flaw has been found in Campcodes Supplier Management System 1.0. Affected by this issue is some unknown functionality of the file /retailer/edit_profile.php. This manipulation of the argument txtRetailerAddress causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2025-15391	A weakness has been identified in D-Link DIR-806A 100CNb11. Affected is the function ssdpcgi_main of the component SSDP Request Handler. This manipulation causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-15373	A security vulnerability has been detected in EyouCMS up to 1.7.7. Impacted is the function saveRemote of the file application/function.php. Such manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor is "[a]cknowledging the existence of the vulnerability, we have completed the fix and will release a new version, v1.7.8".	6.3	More Details
CVE-2025-15453	A security vulnerability has been detected in milvus up to 2.6.7. This vulnerability affects the function expr.Exec of the file pkg/util/expr/expr.go of the component HTTP Endpoint. The manipulation of the argument code leads to deserialization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may	6.3	More Details

	be used. A fix is planned for the next release 2.6.8.		
CVE-2025-15439	A vulnerability was identified in Daptin 0.10.3. Affected by this vulnerability is the function goqu.L of the file server/resource/resource_aggregate.go of the component Aggregate API. The manipulation of the argument column/group/order leads to sql injection. 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-2025-15390	A security flaw has been discovered in PHPGurukul Small CRM 4.0. This impacts an unknown function of the file /admin/edit-user.php. The manipulation results in missing authorization. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2026-0641	A security vulnerability has been detected in TOTOLINK WA300 5.2cu.7112_B20190227. This vulnerability affects the function sub_401510 of the file cstecgi.cgi. The manipulation of the argument UPLOAD_FILENAME leads to command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-0547	A vulnerability was found in PHPGurukul Online Course Registration up to 3.1. This issue affects some unknown processing of the file /admin/edit-student-profile.php of the component Student Registration Page. The manipulation of the argument photo results in unrestricted upload. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-15406	A flaw has been found in PHPGurukul Online Course Registration up to 3.1. This affects an unknown function. This manipulation causes missing authorization. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2025-52516	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. An invalid kernel address dereference in the issimian device driver leads to a denial of service.	6.2	More Details
CVE-2025-13153	The Logo Slider WordPress plugin before 4.9.0 does not validate and escape some of its slider options before outputting them back in the dashboard, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	6.1	More Details
CVE-2025-13456	The ShopBuilder WordPress plugin before 3.2.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2025-67705	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details
CVE-2026-21488	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below are vulnerable to Out-of-bounds Read, Heap-based Buffer Overflow and Improper Null Termination through its CIccTagText::Read function. This issue is fixed in version 2.3.1.2.	6.1	More Details
CVE-2026-21489	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below have Out-of-bounds Read and Integer Underflow (Wrap or Wraparound) vulnerabilities in its CIccCalculatorFunc::SequenceNeedTempReset function. This issue is fixed in version 2.3.1.2.	6.1	More Details
CVE-2025-67704	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details

CVE-2026-21487	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1.1 and below have an Out-of-bounds Read, Use of Out-of-range Pointer Offset and have Improper Input Validation in its CIccProfile::LoadTag function. This issue is fixed in version 2.3.1.2.	6.1	More Details
CVE-2025-67703	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details
CVE-2025-62857	A cross-site scripting (XSS) vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following version: QuMagie 2.8.1 and later	6.1	More Details
CVE-2021-47743	COMMAX Biometric Access Control System 1.0.0 contains an unauthenticated reflected cross-site scripting vulnerability in cookie parameters 'CMX_ADMIN_NM' and 'CMX_COMPLEX_NM'. Attackers can inject malicious HTML and JavaScript code into these cookie values to execute arbitrary scripts in a victim's browser session.	6.1	More Details
CVE-2026-21494	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. A vulnerability present in versions prior to 2.3.1.2 affects users of the iccDEV library who process ICC color profiles. It results in heap buffer overflow in `CIccTagLut8::Validate()`. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.1	More Details
CVE-2025-67710	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details
CVE-2026-21490	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. A vulnerability present in versions prior to 2.3.1.2 affects users of the iccDEV library who process ICC color profiles. It results in heap buffer overflow in `CIccTagLut16::Validate()`. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.1	More Details
CVE-2025-45286	A cross-site scripting (XSS) vulnerability in mccutchen httpbin v2.17.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2026-21491	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. A vulnerability present in versions prior to 2.3.1.2 affects users of the iccDEV library who process ICC color profiles. It results in unicode buffer overflow in `CIccTagTextDescription`. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.1	More Details
CVE-2025-67708	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details
CVE-2025-67709	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated attacker to store files that contain malicious code that may execute in the context of a victim’s browser.	6.1	More Details
CVE-2025-	There is a stored cross site scripting issue in Esri ArcGIS Server 11.4 and earlier on Windows and Linux that in some configurations allows a remote unauthenticated	6.1	More

67711	attacker to store files that contain malicious code that may execute in the context of a victim’s browser.		Details
CVE-2025-62989	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boxy Studio Cooked allows Stored XSS.This issue affects Cooked: from n/a through 1.11.2.	5.9	More Details
CVE-2025-59135	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eLEOPARD Behance Portfolio Manager allows Stored XSS.This issue affects Behance Portfolio Manager: from n/a through 1.7.5.	5.9	More Details
CVE-2025-49355	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ikaes Accessibility Press allows Stored XSS.This issue affects Accessibility Press: from n/a through 1.0.2.	5.9	More Details
CVE-2025-49337	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in janhenckens Dashboard Beacon allows Stored XSS.This issue affects Dashboard Beacon: from n/a through 1.2.0.	5.9	More Details
CVE-2025-62121	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu Logo Slider , Logo Carousel , Logo showcase , Client Logo allows Stored XSS.This issue affects Logo Slider , Logo Carousel , Logo showcase , Client Logo: from n/a through 1.8.1.	5.9	More Details
CVE-2025-62124	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soli WP Post Signature allows Stored XSS.This issue affects WP Post Signature: from n/a through 0.4.1.	5.9	More Details
CVE-2025-62750	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Filipe Seabra WooCommerce Parcelas allows DOM-Based XSS.This issue affects WooCommerce Parcelas: from n/a through 1.3.5.	5.9	More Details
CVE-2025-62149	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SaifuMak Add Custom Codes allows Stored XSS.This issue affects Add Custom Codes: from n/a through 4.80.	5.9	More Details
CVE-2025-62142	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nicashmu Cincopa video and media plugin allows Stored XSS.This issue affects Cincopa video and media plug-in: from n/a through 1.163.	5.9	More Details
CVE-2025-62140	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plainware Locatoraid Store Locator allows Stored XSS.This issue affects Locatoraid Store Locator: from n/a through 3.9.65.	5.9	More Details
CVE-2025-62119	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ViitorCloud Technologies Pvt Ltd Add Featured Image Custom Link allows DOM-Based XSS.This issue affects Add Featured Image Custom Link: from n/a through 2.0.0.	5.9	More Details
CVE-2025-59003	Insertion of Sensitive Information Into Sent Data vulnerability in Inkthemescom Black Rider allows Retrieve Embedded Sensitive Data.This issue affects Black Rider: from n/a through 1.2.3.	5.8	More Details
CVE-2025-67706	ArcGIS Server version 11.5 and earlier on Windows and Linux does not properly validate uploaded files file, which allows remote attackers to upload arbitrary files.	5.6	More Details
CVE-2025-67707	ArcGIS Server version 11.5 and earlier on Windows and Linux does not properly validate uploaded files file, which allows remote attackers to upload arbitrary files.	5.6	More Details
	libtpms, a library that provides software emulation of a Trusted Platform Module, has a		

CVE-2026-21444	flaw in versions 0.10.0 and 0.10.1. The commonly used integration of libtpms with OpenSSL 3.x contained a vulnerability related to the returned IV (initialization vector) when certain symmetric ciphers were used. Instead of returning the last IV it returned the initial IV to the caller, thus weakening the subsequent encryption and decryption steps. The highest threat from this vulnerability is to data confidentiality. Version 0.10.2 fixes the issue. No known workarounds are available.	5.5	More Details
CVE-2026-21492	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a NULL pointer member call vulnerability. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	5.5	More Details
CVE-2025-66157	Missing Authorization vulnerability in merkulove Slider for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Slider for Elementor: from n/a through 1.0.10.	5.4	More Details
CVE-2025-67316	An issue in realme Internet browser v.45.13.4.1 allows a remote attacker to execute arbitrary code via a crafted webpage in the built-in HeyTap/ColorOS browser	5.4	More Details
CVE-2025-62134	Cross-Site Request Forgery (CSRF) vulnerability in A WP Life Contact Form Widget allows Cross Site Request Forgery.This issue affects Contact Form Widget: from n/a through 1.5.1.	5.4	More Details
CVE-2025-62120	Cross-Site Request Forgery (CSRF) vulnerability in Rick Beckman OpenHook allows Cross Site Request Forgery.This issue affects OpenHook: from n/a through 4.3.1.	5.4	More Details
CVE-2025-62117	Cross-Site Request Forgery (CSRF) vulnerability in Jayce53 EasyIndex easyindex allows Cross Site Request Forgery.This issue affects EasyIndex: from n/a through 1.1.1704.	5.4	More Details
CVE-2025-66156	Missing Authorization vulnerability in merkulove Watcher for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Watcher for Elementor: from n/a through 1.0.9.	5.4	More Details
CVE-2025-66155	Missing Authorization vulnerability in merkulove Questionar for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Questionar for Elementor: from n/a through 1.1.7.	5.4	More Details
CVE-2025-66148	Missing Authorization vulnerability in merkulove Conformer for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Conformer for Elementor: from n/a through 1.0.7.	5.4	More Details
CVE-2021-47725	STVS ProVision 5.9.10 contains a cross-site scripting vulnerability in the 'files' POST parameter that allows authenticated attackers to inject arbitrary HTML code. Attackers can exploit the unvalidated input to execute malicious scripts within a user's browser session in the context of the affected site.	5.4	More Details
CVE-2025-66154	Missing Authorization vulnerability in merkulove Couponer for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Couponer for Elementor: from n/a through 1.1.7.	5.4	More Details
CVE-2025-62088	Server-Side Request Forgery (SSRF) vulnerability in extendons WordPress & WooCommerce Scraper Plugin, Import Data from Any Site allows Server Side Request Forgery.This issue affects WordPress & WooCommerce Scraper Plugin, Import Data from Any Site: from n/a through 1.0.7.	5.4	More Details
CVE-2025-69345	Missing Authorization vulnerability in BoldGrid Post and Page Builder by BoldGrid post-and-page-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post and Page Builder by BoldGrid: from n/a through <=	5.4	More Details

	1.27.9.		
CVE-2025-69354	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-2025-69353	Missing Authorization vulnerability in Proxy &amp; VPN Blocker Proxy &amp; VPN Blocker proxy-vpn-blocker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Proxy &amp; VPN Blocker: from n/a through <= 3.5.3.	5.4	More Details
CVE-2025-69346	Missing Authorization vulnerability in WPCenter AffiliateX affiliatex allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AffiliateX: from n/a through <= 1.3.9.3.	5.4	More Details
CVE-2025-69352	Missing Authorization vulnerability in StellarWP The Events Calendar the-events-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Events Calendar: from n/a through <= 6.15.12.2.	5.4	More Details
CVE-2025-62888	Missing Authorization vulnerability in Marco Milesi WP Attachments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Attachments: from n/a through 5.2.	5.4	More Details
CVE-2025-67315	Cross Site Request Forgery vulnerability in Employee Leave Management System v.2.1 allows a remote attacker to escalate privileges via the manage-employee.php component	5.4	More Details
CVE-2025-69349	Missing Authorization vulnerability in Fahad Mahmood RSS Feed Widget rss-feed-widget allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RSS Feed Widget: from n/a through <= 3.0.2.	5.4	More Details
CVE-2025-66149	Missing Authorization vulnerability in merkulove UnGrabber allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UnGrabber: from n/a through 3.1.3.	5.4	More Details
CVE-2025-66158	Missing Authorization vulnerability in merkulove Gmaper for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gmaper for Elementor: from n/a through 1.0.9.	5.4	More Details
CVE-2025-66150	Missing Authorization vulnerability in merkulove Appender allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Appender: from n/a through 1.1.1.	5.4	More Details
CVE-2025-66151	Missing Authorization vulnerability in merkulove Countdowner for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Countdowner for Elementor: from n/a through 1.0.4.	5.4	More Details
CVE-2023-52212	Cross-Site Request Forgery (CSRF) vulnerability in Automattic WP Job Manager allows Cross Site Request Forgery.This issue affects WP Job Manager: from n/a through 2.0.0.	5.4	More Details
CVE-2025-66152	Missing Authorization vulnerability in merkulove Criptopayer for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Criptopayer for Elementor: from n/a through 1.0.1.	5.4	More Details
CVE-2025-66153	Missing Authorization vulnerability in merkulove Headinger for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Headinger for Elementor: from n/a through 1.1.4.	5.4	More Details
CVE-2025-	A vulnerability was determined in cld378632668 JavaMall up to 994f1e2b019378ec9444cdf3fce2d5b5f72d28f0. Affected is the function delete of the file src/main/java/com/macro/mall/controller/MinioController.java. This manipulation of the argument objectName causes path traversal. The attack can be initiated remotely.	5.4	More Details

15449	Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-66144	Missing Authorization vulnerability in merkulove Worker for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Worker for Elementor: from n/a through 1.0.10.	5.4	More Details
CVE-2025-66145	Missing Authorization vulnerability in merkulove Worker for WPBakery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Worker for WPBakery: from n/a through 1.1.1.	5.4	More Details
CVE-2025-66146	Missing Authorization vulnerability in merkulove Logger for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Logger for Elementor: from n/a through 1.0.9.	5.4	More Details
CVE-2025-62144	Missing Authorization vulnerability in Mohammed Kaludi Core Web Vitals & PageSpeed Booster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Core Web Vitals & PageSpeed Booster: from n/a through 1.0.27.	5.4	More Details
CVE-2025-69348	Missing Authorization vulnerability in CoolHappy The Events Calendar Countdown Addon countdown-for-the-events-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Events Calendar Countdown Addon: from n/a through <= 1.4.15.	5.4	More Details
CVE-2025-62091	Missing Authorization vulnerability in Vollstart Serial Codes Generator and Validator with WooCommerce Support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Serial Codes Generator and Validator with WooCommerce Support: from n/a through 2.8.2.	5.4	More Details
CVE-2025-62098	Missing Authorization vulnerability in Totalsoft Portfolio Gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Portfolio Gallery: from n/a through 1.4.8.	5.4	More Details
CVE-2025-13766	The MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin for WordPress is vulnerable to unauthorized modification and deletion of data due to a missing capability checks on multiple REST API endpoints in all versions up to, and including, 3.7.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload or delete arbitrary media files, delete or modify posts, and create/manage course templates	5.4	More Details
CVE-2025-69341	Missing Authorization vulnerability in BuddhaThemes WeDesignTech Ultimate Booking Addon wedesigntech-ultimate-booking-addon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WeDesignTech Ultimate Booking Addon: from n/a through <= 1.0.3.	5.4	More Details
CVE-2025-66159	Missing Authorization vulnerability in merkulove Walker for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Walker for Elementor: from n/a through 1.1.6.	5.4	More Details
CVE-2025-66160	Missing Authorization vulnerability in merkulove Select Graphist for Elementor Graphist for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Select Graphist for Elementor Graphist for Elementor: from n/a through 1.2.10.	5.4	More Details
CVE-2025-62108	Missing Authorization vulnerability in SaifuMak Add Custom Codes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Add Custom Codes: from n/a through 4.80.	5.4	More Details
CVE-2025-62116	Missing Authorization vulnerability in Quadlayers AI Copilot allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Copilot: from n/a through 1.4.7.	5.3	More Details

CVE-2025-62129	Missing Authorization vulnerability in Magnigenie RestroPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RestroPress: from n/a through 3.2.4.2.	5.3	More Details
CVE-2025-62126	Insertion of Sensitive Information Into Sent Data vulnerability in Razvan Stanga Varnish/Nginx Proxy Caching allows Retrieve Embedded Sensitive Data.This issue affects Varnish/Nginx Proxy Caching: from n/a through 1.8.3.	5.3	More Details
CVE-2020-36908	SnapGear Management Console SG560 version 3.1.5 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without user consent. Attackers can craft a malicious web page that automatically submits a form to create a new super user account with full administrative privileges when a logged-in user visits the page.	5.3	More Details
CVE-2025-62122	Missing Authorization vulnerability in Solwininfotech Trash Duplicate and 301 Redirect allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Trash Duplicate and 301 Redirect: from n/a through 1.9.1.	5.3	More Details
CVE-2025-15412	A security vulnerability has been detected in WebAssembly wabt up to 1.0.39. This issue affects the function wabt::Decompiler::VarName of the file /src/repro/wabt/bin/wasm-decompile of the component wasm-decompile. Such manipulation leads to out-of-bounds read. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. Unfortunately, the project has no active maintainer at the moment. In a reply to the issue report somebody recommended to the researcher to provide a PR himself.	5.3	More Details
CVE-2025-62114	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Marcelo Torres Download Media Library allows Retrieve Embedded Sensitive Data.This issue affects Download Media Library: from n/a through 0.2.1.	5.3	More Details
CVE-2025-62092	Missing Authorization vulnerability in Wiremo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wiremo: from n/a through 1.4.99.	5.3	More Details
CVE-2025-3654	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains an information disclosure vulnerability that allows unauthorized access to device hardware information by exploiting insecure API endpoints. Attackers can retrieve device serial numbers and MAC addresses through /device/devicePetRelation/getBoundDevices using pet IDs, enabling full device control without proper authorization checks.	5.3	More Details
CVE-2025-68273	Signal K Server is a server application that runs on a central hub in a boat. An unauthenticated information disclosure vulnerability in versions prior to 2.19.0 allows any user to retrieve sensitive system information, including the full SignalK data schema, connected serial devices, and installed analyzer tools. This exposure facilitates reconnaissance for further attacks. Version 2.19.0 patches the issue.	5.3	More Details
CVE-2025-3652	Petlibro Smart Pet Feeder Platform versions up to 1.7.31 contains an information disclosure vulnerability that allows unauthorized access to private audio recordings by exploiting sequential audio IDs and insecure assignment endpoints. Attackers can send requests to /device/deviceAudio/use with arbitrary audio IDs to assign recordings to any device, then retrieve audio URLs to access other users' private recordings.	5.3	More Details
CVE-2026-21635	An Improper Access Control could allow a malicious actor in Wi-Fi range to the EV Station Lite (v1.5.2 and earlier) to use WiFi AutoLink feature on a device that was only adopted via Ethernet.	5.3	More Details
CVE-2025-15411	A weakness has been identified in WebAssembly wabt up to 1.0.39. This vulnerability affects the function wabt::AST::InsertNode of the file /src/repro/wabt/bin/wasm-decompile of the component wasm-decompile. This manipulation causes memory corruption. 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. Unfortunately, the project has no active maintainer at the moment. In a reply to the issue report somebody	5.3	More Details

	recommended to the researcher to provide a PR himself.		
CVE-2025-62081	Missing Authorization vulnerability in Channelize.Io Team Live Shopping & Shoppable Videos For WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Live Shopping & Shoppable Videos For WooCommerce: from n/a through 2.2.0.	5.3	More Details
CVE-2025-62141	Missing Authorization vulnerability in 101gen Wawp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wawp: from n/a through 4.0.5.	5.3	More Details
CVE-2025-62145	Missing Authorization vulnerability in NewClarity DMCA Protection Badge allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DMCA Protection Badge: from n/a through 2.2.0.	5.3	More Details
CVE-2025-15413	A vulnerability was detected in wasm3 up to 0.5.0. Impacted is the function op_SetSlot_i32/op_CallIndirect of the file m3_exec.h. Performing manipulation results in memory corruption. The attack needs to be approached locally. The exploit is now public and may be used. Unfortunately, the project has no active maintainer at the moment.	5.3	More Details
CVE-2025-14441	The Popupkit plugin for WordPress is vulnerable to arbitrary subscriber data deletion due to missing authorization on the DELETE `/subscribers` REST API endpoint in all versions up to, and including, 2.2.0. This is due to the `permission_callback` only validating wp_rest nonce without checking user capabilities. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary subscriber records.	5.3	More Details
CVE-2025-13820	The Comments WordPress plugin before 7.6.40 does not properly validate user's identity when using the disqus.com provider, allowing an attacker to log in to any user (when knowing their email address) when such user does not have an account on disqus.com yet.	5.3	More Details
CVE-2025-69413	In Gitea before 1.25.2, /api/v1/user has different responses for failed authentication depending on whether a username exists.	5.3	More Details
CVE-2020-36913	All-Dynamics Software enlogic:show 2.0.2 contains a session fixation vulnerability that allows attackers to set a predefined PHP session identifier during the login process. Attackers can forge HTTP GET requests to welcome.php with a manipulated session token to bypass authentication and potentially execute cross-site request forgery attacks.	5.3	More Details
CVE-2025-13215	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.17.13 via the auxels_ajax_search due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract titles of draft posts that they should not have access to.	5.3	More Details
CVE-2025-62747	Missing Authorization vulnerability in Aum Watcharapon Featured Image Generator allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Featured Image Generator: from n/a through 1.3.3.	5.3	More Details
CVE-2025-62139	Insertion of Sensitive Information Into Sent Data vulnerability in Vladimir Statsenko Terms descriptions allows Retrieve Embedded Sensitive Data.This issue affects Terms descriptions: from n/a through 3.4.9.	5.3	More Details
CVE-2025-12519	Missing Authorization vulnerability in Centreon Infra Monitoring (Administration parameters API endpoint modules) allows Accessing Functionality Not Properly Constrained by ACLs, resulting in Information Disclosure like downtime or acknowledgement configurations. This issue affects Infra Monitoring: from 25.10.0 before 25.10.2, from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19.	5.3	More Details

CVE-2025-62755	Unauthenticated Broken Access Control in GS Portfolio for Envato <= 1.4.2 versions.	5.3	More Details
CVE-2025-13964	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the catch_lp_ajax function in all versions up to, and including, 4.3.2. This makes it possible for unauthenticated attackers to modify course contents by adding/removing/updating/re-ordering sections or modifying section items.	5.3	More Details
CVE-2025-49349	Missing Authorization vulnerability in Reuters News Agency Reuters Direct allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Reuters Direct: from n/a through 3.0.0.	5.3	More Details
CVE-2025-62079	Missing Authorization vulnerability in Damian WP Export Categories & Taxonomies allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Export Categories &amp; Taxonomies: from n/a through 1.0.3.	5.3	More Details
CVE-2025-49334	Authorization Bypass Through User-Controlled Key vulnerability in Eduardo Villão MyD Delivery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MyD Delivery: from n/a through 1.3.7.	5.3	More Details
CVE-2025-14434	The Ultimate Post Kit Addons for Elementor WordPress plugin before 4.0.16 exposes multiple AJAX “load more” endpoints such as upk_alex_grid_loadmore_posts without ensuring that posts to be displayed are published authentication. This allows an unauthenticated attacker to query arbitrary posts and retrieve rendered HTML content of private and unpublished ones.	5.3	More Details
CVE-2024-55374	REDCap 14.3.13 allows an attacker to enumerate usernames due to an observable discrepancy between login attempts.	5.3	More Details
CVE-2025-63053	Authorization Bypass Through User-Controlled Key vulnerability in Jewel Theme Master Addons for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Master Addons for Elementor: from n/a through 2.0.9.9.4.	5.3	More Details
CVE-2025-15432	A vulnerability has been found in yeqifu carRental up to 3fabb7eae93d209426638863980301d6f99866b3. This vulnerability affects the function downloadShowFile of the file /file/downloadShowFile.action of the component com.yeqifu.sys.controller.FileController. The manipulation of the argument path leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2025-62138	Missing Authorization vulnerability in CedCommerce WP Advanced PDF allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Advanced PDF: from n/a through 1.1.7.	5.3	More Details
CVE-2025-49338	Missing Authorization vulnerability in Flowbox allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flowbox: from n/a through 1.1.5.	5.3	More Details
CVE-2025-11370	The Popup and Slider Builder by Depicter – Add Email collecting Popup, Popup Modal, Coupon Popup, Image Slider, Carousel Slider, Post Slider Carousel plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'store' function of the RulesAjaxController class in all versions up to, and including, 4.0.7. This makes it possible for unauthenticated attackers to update pop-up display settings.	5.3	More Details
CVE-	The Ninja Forms WordPress plugin before 3.13.3 allows unauthenticated attackers to		

2025-14072	generate valid access tokens via the REST API which can then be used to read form submissions.	5.3	More Details
CVE-2025-59136	Insertion of Sensitive Information Into Sent Data vulnerability in Efí Bank Gerencianet Oficial allows Retrieve Embedded Sensitive Data.This issue affects Gerencianet Oficial: from n/a through 3.1.3.	5.3	More Details
CVE-2025-63031	Missing Authorization vulnerability in WP Grids EasyTest allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EasyTest: from n/a through 1.0.1.	5.3	More Details
CVE-2025-63016	Missing Authorization vulnerability in Quadlayers QuadLayers TikTok Feed allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects QuadLayers TikTok Feed: from n/a through 4.6.4.	5.3	More Details
CVE-2025-14047	The Registration, User Profile, Membership, Content Restriction, User Directory, and Frontend Post Submission – WP User Frontend plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'Frontend_Form_Ajax::submit_post' function in all versions up to, and including, 4.2.4. This makes it possible for unauthenticated attackers to delete attachment.	5.3	More Details
CVE-2025-14034	The ilGhera Support System for WooCommerce plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'delete_single_ticket_callback' and 'change_ticket_status_callback' functions in all versions up to, and including, 1.2.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary support tickets and modify their status.	5.3	More Details
CVE-2026-21484	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to commit e287fab56089cf8fcea9ba579a3ecdeca0daa313, the password recovery endpoint returns different error messages depending on whether a username exists, so enabling username enumeration. Commit e287fab56089cf8fcea9ba579a3ecdeca0daa313 fixes this issue.	5.3	More Details
CVE-2025-62147	Missing Authorization vulnerability in Nik Melnik Realbig allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Realbig: from n/a through 1.1.3.	5.3	More Details
CVE-2025-63001	Missing Authorization vulnerability in nicdark Hotel Booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hotel Booking: from n/a through 3.8.	5.3	More Details
CVE-2025-15422	A flaw has been found in EmpireSoft EmpireCMS up to 8.0. This issue affects the function egetip of the file e/class/connect.php of the component IP Address Handler. This manipulation causes protection mechanism failure. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-63022	Missing Authorization vulnerability in Illia Simple Like Page allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simple Like Page: from n/a through 1.5.3.	5.3	More Details
CVE-2025-52515	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. A race condition in the issimian device driver results in an out-of-bounds access, leading to a denial of service.	5.1	More Details
CVE-2025-69416	In the plex.tv backend for Plex Media Server (PMS) through 2025-12-31, a non-server device token can retrieve other tokens (intended for unrelated access) via clients.plex.tv/devices.xml.	5.0	More Details

CVE-2025-69417	In the plex.tv backend for Plex Media Server (PMS) through 2025-12-31, a non-server device token can retrieve share tokens (intended for unrelated access) via a shared_servers endpoint.	5.0	More Details
CVE-2025-53590	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: QTS 5.2.7.3256 build 20250913 and later	4.9	More Details
CVE-2025-59138	Server-Side Request Forgery (SSRF) vulnerability in Jthemes Genemy allows Server Side Request Forgery.This issue affects Genemy: from n/a through 1.6.6.	4.9	More Details
CVE-2025-52431	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-53596	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-52430	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-52426	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-53589	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-59380	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3332 build 20251128 and later QuTS hero h5.2.8.3321 build 20251117 and later	4.9	More Details
CVE-2025-53414	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details

CVE-2025-54166	An out-of-bounds read vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-53405	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-57705	An allocation of resources without limits or throttling vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-54164	An out-of-bounds read vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-13409	The Form Vibes – Database Manager for Forms plugin for WordPress is vulnerable to SQL Injection via the 'params' parameter in all versions up to, and including, 1.4.13 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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-2025-54165	An out-of-bounds read vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3256 build 20250913 and later QuTS hero h5.2.7.3256 build 20250913 and later QuTS hero h5.3.1.3250 build 20250912 and later	4.9	More Details
CVE-2025-59381	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3332 build 20251128 and later QuTS hero h5.2.8.3321 build 20251117 and later	4.9	More Details
CVE-2025-14830	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in JFrog Artifactory (Workers) allows Cross-Site Scripting (XSS).This issue affects Artifactory (Workers): from >=7.94.0 through <7.117.10.	4.9	More Details
CVE-2025-15414	A flaw has been found in go-sonic sonic up to 1.1.4. The affected element is the function FetchTheme of the file service/theme/git_fetcher.go of the component Theme Fetching API. Executing manipulation of the argument uri can lead to server-side request forgery. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-	A security vulnerability has been detected in code-projects Content Management System 1.0. Impacted is an unknown function of the file /admin/edit_posts.php. The manipulation of the argument image leads to unrestricted upload. The attack is possible	4.7	More Details

0566	to be carried out remotely. The exploit has been disclosed publicly and may be used.		
CVE-2023-7331	A vulnerability was detected in PKrystian Full-Stack-Bank up to bf73a0179e3ff07c0d7dc35297cea0be0e5b1317. This vulnerability affects unknown code of the component User Handler. Performing manipulation results in sql injection. It is possible to initiate the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 25c9965a872c704f3a9475488dc5d3196902199a. It is suggested to install a patch to address this issue.	4.7	More Details
CVE-2025-15415	A vulnerability has been found in xnx3 wangmarket up to 6.4. The impacted element is the function uploadImage of the file /sits/uploadImage.do of the component XML File Handler. The manipulation of the argument image leads to unrestricted upload. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-15443	A vulnerability was identified in CRMEB up to 5.6.1. This issue affects some unknown processing of the file /adminapi/product/product_export. Such manipulation of the argument cate_id leads to sql injection. 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.	4.7	More Details
CVE-2025-15438	A vulnerability was determined in PluXml up to 5.8.22. Affected is the function FileCookieJar::__destruct of the file core/admin/medias.php of the component Media Management Module. Executing manipulation of the argument File can lead to deserialization. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was informed early about this issue and announced that "[w]e fix this issue in the next version 5.8.23". A patch for it is ready.	4.7	More Details
CVE-2025-15442	A vulnerability was determined in CRMEB up to 5.6.1. This vulnerability affects unknown code of the file /adminapi/export/product_list. This manipulation of the argument cate_id causes sql injection. 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.	4.7	More Details
CVE-2025-15394	A vulnerability was detected in iCMS up to 8.0.0. Affected is the function Save of the file app/config/ConfigAdmincp.php of the component POST Parameter Handler. The manipulation of the argument config results in code injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-69277	libsodium before ad3004e, in atypical use cases involving certain custom cryptography or untrusted data to crypto_core_ed25519_is_valid_point, mishandles checks for whether an elliptic curve point is valid because it sometimes allows points that aren't in the main cryptographic group.	4.5	More Details
CVE-2026-0571	A security flaw has been discovered in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. Affected by this issue is the function createResponseEntity of the file warehouse\src\main\java\com\yeqifu\sys\common\AppFileUtils.java. The manipulation of the argument path results in path traversal. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	4.3	More Details
CVE-2025-7048	On affected platforms running Arista EOS with MACsec configuration, a specially crafted packet can cause the MACsec process to terminate unexpectedly. Continuous receipt of these packets with certain MACsec configurations can cause longer term disruption of dataplane traffic.	4.3	More Details

CVE-2025-62099	Missing Authorization vulnerability in Approveme Signature Add-On for Gravity Forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Signature Add-On for Gravity Forms: from n/a through 1.8.6.	4.3	More Details
CVE-2025-62101	Cross-Site Request Forgery (CSRF) vulnerability in Omid Shamloo Pardakht Delkhah allows Cross Site Request Forgery.This issue affects Pardakht Delkhah: from n/a through 3.0.0.	4.3	More Details
CVE-2025-14783	The Easy Digital Downloads plugin for WordPress is vulnerable to Unvalidated Redirect in all versions up to, and including, 3.6.2. This is due to insufficient validation on the redirect url supplied via the 'edd_redirect' parameter. This makes it possible for unauthenticated attackers to redirect users with the password reset email to potentially malicious sites if they can successfully trick them into performing an action.	4.3	More Details
CVE-2025-62113	Cross-Site Request Forgery (CSRF) vulnerability in emendo_seb Co-marquage service-public.Fr allows Cross Site Request Forgery.This issue affects Co-marquage service-public.Fr: from n/a through 0.5.77.	4.3	More Details
CVE-2025-62115	Missing Authorization vulnerability in ThemeBoy Hide Plugins allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hide Plugins: from n/a through 1.0.4.	4.3	More Details
CVE-2025-62123	Cross-Site Request Forgery (CSRF) vulnerability in Ink themes WP Gmail SMTP allows Cross Site Request Forgery.This issue affects WP Gmail SMTP: from n/a through 1.0.7.	4.3	More Details
CVE-2025-62874	Missing Authorization vulnerability in Alexander AnyComment allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AnyComment: from n/a through 0.3.6.	4.3	More Details
CVE-2025-63038	Missing Authorization vulnerability in Northern Beaches Websites WP Custom Admin Interface allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Custom Admin Interface: from n/a through 7.40.	4.3	More Details
CVE-2025-15237	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has a Path Traversal vulnerability, allowing authenticated remote attackers to read folder names under the specified path by exploiting an Absolute Path Traversal vulnerability.	4.3	More Details
CVE-2025-15223	A vulnerability was found in Philipinho Simple-PHP-Blog up to 94b5d3e57308bce5dfbc44c3edafa9811893d958. Impacted is an unknown function of the file /login.php. Performing manipulation of the argument Username results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could 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 vendor was contacted early about this disclosure and makes clear that the product is "[f]or educational purposes only".	4.3	More Details
CVE-2025-15236	QOCA aim AI Medical Cloud Platform developed by Quanta Computer has a Path Traversal vulnerability, allowing authenticated remote attackers to read folder names under the specified path by exploiting an Absolute Path Traversal vulnerability.	4.3	More Details
CVE-2025-9294	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the qsm_dashboard_delete_result function in all versions up to, and including, 10.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete quiz results.	4.3	More Details
CVE-2025-62143	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in nicashmu Post Video Players allows Retrieve Embedded Sensitive Data.This issue affects Post Video Players: from n/a through 1.163.	4.3	More Details

CVE-2025-65922	PLANKA 2.0.0 lacks X-Frame-Options and CSP frame-ancestors headers, allowing the application to be embedded within malicious iframes. While this does not lead to unintended modification of projects or tasks, it exposes users to Phishing attacks. Attackers can frame the legitimate Planka application on a malicious site to establish false trust (UI Redressing), potentially tricking users into entering sensitive information or credentials into overlaid fake forms. NOTE: this is disputed by the Supplier because "PLANKA uses SameSite=Strict cookies, preventing authentication in cross-origin contexts. No session can be established. No credential interception or unauthorized actions are possible. Browser Same-Origin Policy prevents the parent page from accessing iframe content. Clickjacking is not applicable on the login page. Any credential capture would require attacker-controlled input and user interaction equivalent to phishing. The security outcome depends entirely on the user's trust in the parent page. An attacker can achieve the same effect with a fully fake login page. Embedding the legitimate page adds no risk, as browsers do not show URL, certificate, or padlock indicators in cross-origin iframes."	4.3	More Details
CVE-2025-62154	Missing Authorization vulnerability in Recorp AI Content Writing Assistant (Content Writer, ChatGPT, Image Generator) All in One allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Content Writing Assistant (Content Writer, ChatGPT, Image Generator) All in One: from n/a through 1.1.7.	4.3	More Details
CVE-2025-62150	Missing Authorization vulnerability in Themesawesome History Timeline allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects History Timeline: from n/a through 1.0.6.	4.3	More Details
CVE-2025-62148	Cross-Site Request Forgery (CSRF) vulnerability in Eugen Bobrowski Robots.Txt rewrite allows Cross Site Request Forgery.This issue affects Robots.Txt rewrite: from n/a through 1.6.1.	4.3	More Details
CVE-2025-15405	A vulnerability was detected in PHPEMS up to 11.0. The impacted element is an unknown function. The manipulation results in cross-site request forgery. The attack may be launched remotely.	4.3	More Details
CVE-2025-62133	Cross-Site Request Forgery (CSRF) vulnerability in Manidoraisamy FormFacade allows Cross Site Request Forgery.This issue affects FormFacade: from n/a through 1.4.1.	4.3	More Details
CVE-2025-62132	Missing Authorization vulnerability in Strategy11 Team Tasty Recipes Lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tasty Recipes Lite: from n/a through 1.1.5.	4.3	More Details
CVE-2025-62131	Missing Authorization vulnerability in Strategy11 Team Tasty Recipes Lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tasty Recipes Lite: from n/a through 1.1.5.	4.3	More Details
CVE-2025-62130	Missing Authorization vulnerability in WPdiscover Accordion Slider Gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Accordion Slider Gallery: from n/a through 2.7.	4.3	More Details
CVE-2025-53344	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress Thim Core allows Cross Site Request Forgery.This issue affects Thim Core: from n/a through 2.3.3.	4.3	More Details
CVE-2025-62089	Cross-Site Request Forgery (CSRF) vulnerability in MERGADO Mergado Pack allows Cross Site Request Forgery.This issue affects Mergado Pack: from n/a through 4.2.0.	4.3	More Details
CVE-2020-36918	iDS6 DSSPro Digital Signage System 6.2 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without request validation. Attackers can craft malicious web pages to trick logged-in administrators into adding unauthorized users by exploiting the lack of CSRF protections.	4.3	More Details

CVE-2025-62087	Missing Authorization vulnerability in Web Builder 143 Sticky Notes for WP Dashboard allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sticky Notes for WP Dashboard: from n/a through 1.2.4.	4.3	More Details
CVE-2025-62084	Cross-Site Request Forgery (CSRF) vulnerability in Imdad Next Web iNext Woo Pincode Checker allows Cross Site Request Forgery.This issue affects iNext Woo Pincode Checker: from n/a through 2.3.1.	4.3	More Details
CVE-2025-62080	Cross-Site Request Forgery (CSRF) vulnerability in Channelize.Io Team Live Shopping & Shoppable Videos For WooCommerce allows Cross Site Request Forgery.This issue affects Live Shopping & Shoppable Videos For WooCommerce: from n/a through 2.2.0.	4.3	More Details
CVE-2025-59130	Cross-Site Request Forgery (CSRF) vulnerability in Appointify allows Cross Site Request Forgery.This issue affects Appointify: from n/a through 1.0.8.	4.3	More Details
CVE-2025-49356	Missing Authorization vulnerability in Mykola Lukin Orders Chat for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Orders Chat for WooCommerce: from n/a through 1.2.0.	4.3	More Details
CVE-2020-36906	P5 FNIP-8x16A FNIP-4xSH 1.0.20 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without user consent. Attackers can craft malicious web pages to add new admin users, change passwords, and modify system configurations by tricking authenticated users into loading a specially crafted form.	4.3	More Details
CVE-2025-69284	Plane is an an open-source project management tool. In plane.io, a guest user doesn't have a permission to access https[:]//app[.]plane[.]so/[:]slug/settings. Prior to Plane version 1.2.0, a problem occurs when the `/api/workspaces/:slug/members/` is accessible by guest and able to list of users on a specific workspace that they joined. Since the `display_name` in the response is actually the handler of the email, a malicious guest can still identify admin users' email addresses. Version 1.2.0 fixes this issue.	4.3	More Details
CVE-2025-13812	The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the gamipress_ajax_get_posts and gamipress_ajax_get_users functions in all versions up to, and including, 7.6.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enumerate users, including their email addresses and to retrieve titles of private posts.	4.3	More Details
CVE-2025-14371	The Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the taxopress_ai_add_post_term function in all versions up to, and including, 3.41.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to add or remove taxonomy terms (tags, categories) on any post, including ones they do not own.	4.3	More Details
CVE-2025-62751	Missing Authorization vulnerability in Extend Themes Vireo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Vireo: from n/a through 1.0.24.	4.3	More Details
CVE-2025-14428	The All-in-one Sticky Floating Contact Form, Call, Click to Chat, and 50+ Social Icon Tabs - My Sticky Elements plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the 'my_sticky_elements_bulks' function in all versions up to, and including, 2.3.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all contact form leads stored by the plugin.	4.3	More Details
CVE-	Missing Authorization vulnerability in Fahad Mahmood Easy Upload Files During		More

2025-62078	Checkout allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Upload Files During Checkout: from n/a through 3.0.0.	4.3	Details
CVE-2026-0586	A vulnerability was detected in code-projects Online Product Reservation System 1.0. The affected element is an unknown function of the file handgunner-administrator/prod.php. Performing a manipulation of the argument cat results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-63004	Missing Authorization vulnerability in Skynet Technologies USA LLC All in One Accessibility allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects All in One Accessibility: from n/a through 1.14.	4.3	More Details
CVE-2025-31046	Missing Authorization vulnerability in WPvibes AnyWhere Elementor Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AnyWhere Elementor Pro: from n/a through 2.29.	4.3	More Details
CVE-2025-63014	Cross-Site Request Forgery (CSRF) vulnerability in Serhii Pasyuk Gmedia Photo Gallery allows Cross Site Request Forgery.This issue affects Gmedia Photo Gallery: from n/a through 1.24.1.	4.3	More Details
CVE-2025-62083	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WP Messiah BoomDevs WordPress Coming Soon Plugin allows Retrieve Embedded Sensitive Data.This issue affects BoomDevs WordPress Coming Soon Plugin: from n/a through 1.0.4.	4.3	More Details
CVE-2025-69336	Missing Authorization vulnerability in bdthemes Ultimate Store Kit Elementor Addons ultimate-store-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Store Kit Elementor Addons: from n/a through <= 2.9.4.	4.3	More Details
CVE-2025-63040	Cross-Site Request Forgery (CSRF) vulnerability in Saad Iqbal Post Snippets allows Cross Site Request Forgery.This issue affects Post Snippets: from n/a through 4.0.11.	4.3	More Details
CVE-2025-69331	Missing Authorization vulnerability in Jeroen Schmit Theater for WordPress theatre allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Theater for WordPress: from n/a through <= 0.19.	4.3	More Details
CVE-2025-69327	Missing Authorization vulnerability in magepeopleteam Car Rental Manager car-rental-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Car Rental Manager: from n/a through <= 1.0.9.	4.3	More Details
CVE-2025-49339	Missing Authorization vulnerability in Digages Direct Payments WP allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Direct Payments WP: from n/a through 1.3.0.	4.3	More Details
CVE-2025-49352	Authorization Bypass Through User-Controlled Key vulnerability in YoOhw Studio Order Cancellation & Returns for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Order Cancellation & Returns for WooCommerce: from n/a through 1.1.10.	4.3	More Details
CVE-2025-49340	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Digages Direct Payments WP allows Retrieve Embedded Sensitive Data.This issue affects Direct Payments WP: from n/a through 1.3.0.	4.3	More Details
CVE-2025-15398	A security vulnerability has been detected in Uasoft badaso up to 2.9.7. Affected is the function forgetPassword of the file src/Controllers/BadasoAuthController.php of the component Token Handler. Such manipulation leads to weak password recovery. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is told to be 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	3.7	More Details

	way.		
CVE-2026-0587	A security flaw has been discovered in Xinhu Rainrock RockOA up to 2.7.1. Affected is an unknown function of the file rock_page_gong.php of the component Cover Image Handler. The manipulation of the argument fengmian results in cross site scripting. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-0588	A weakness has been identified in Xinhu Rainrock RockOA up to 2.7.1. Affected by this vulnerability is an unknown functionality of the file rockfun.php of the component API. This manipulation of the argument callback causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-9543	The FlexTable WordPress plugin before 3.19.2 does not sanitise and escape the imported links from Google Sheet cells, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	3.5	More Details
CVE-2025-15374	A vulnerability was detected in EyouCMS up to 1.7.7. The affected element is an unknown function of the file application/home/model/Ask.php of the component Ask Module. Performing manipulation of the argument content results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used. The vendor is "[a]cknowledging the existence of the vulnerability, we have completed the fix and will release a new version, v1.7.8".	3.5	More Details
CVE-2025-15437	A vulnerability was found in LigeroSmart up to 6.1.24. This affects an unknown part of the component Environment Variable Handler. Performing manipulation of the argument REQUEST_URI results in cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used. Upgrading to version 6.1.26 and 6.3 is able to mitigate this issue. The patch is named 264ac5b2be5b3c673ebd8cb862e673f5d300d9a7. The affected component should be upgraded.	3.5	More Details
CVE-2026-0580	A vulnerability was found in SourceCodester API Key Manager App 1.0. Affected by this vulnerability is an unknown functionality of the component Import Key Handler. Performing a manipulation results in cross site scripting. The attack can be initiated remotely.	3.5	More Details
CVE-2019-25262	A security vulnerability has been detected in elinicksic Razgover up to db37dfc5c82f023a40f2f7834ded6633fb2b5262. This affects an unknown part of the file Chattify/send.php of the component Chat Message Handler. Such manipulation of the argument msg leads to cross site scripting. The attack may be performed from remote. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The name of the patch is 995dd89d0e3ec5522966724be23a5d58ca1bdac3. Applying a patch is advised to resolve this issue. This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-69412	KDE messagelib before 25.11.90 ignores SSL errors for threatMatches:find in the Google Safe Browsing Lookup API (aka phishing API), which might allow spoofing of threat data. NOTE: this Lookup API is not contacted in the messagelib default configuration.	3.4	More Details
CVE-2025-15418	A security flaw has been discovered in Open5GS up to 2.7.6. Affected by this vulnerability is the function ogs_gtp2_parse_bearer_qos in the library lib/gtp/v2/types.c of the component Bearer QoS IE Length Handler. Performing manipulation results in denial of service. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The patch is named 4e913d21f2c032b187815f063dbab5ebe65fe83a. To fix this issue, it is recommended to	3.3	More Details

	deploy a patch.		
CVE-2025-15417	A vulnerability was identified in Open5GS up to 2.7.6. Affected is the function sgwc_s11_handle_create_session_request of the file src/sgwc/s11-handler.c of the component GTPv2-C F-TEID Handler. Such manipulation leads to denial of service. The attack must be carried out locally. The exploit is publicly available and might be used. The name of the patch is 465273d13ba5d47b274c38c9d1b07f04859178a1. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-21674	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below contain a memory leak vulnerability in its XML MPE Parsing Path (iccFromXml). This issue is fixed in version 2.3.1.1.	3.3	More Details
CVE-2025-15419	A weakness has been identified in Open5GS up to 2.7.6. Affected by this issue is the function sgwc_s5c_handle_create_session_response of the file src/sgwc/s5c-handler.c of the component GTPv2-C Flow Handler. Executing a manipulation can lead to denial of service. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. This patch is called 5aaa09907e7b9e0a326265a5f08d56f54280b5f2. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2025-15454	A vulnerability was detected in zhanglun lettura up to 0.1.22. This issue affects some unknown processing of the file src/components/ArticleView/ContentRender.tsx of the component RSS Handler. The manipulation results in cross site scripting. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit is now public and may be used. The patch is identified as 67213093db9923e828a6e3fd8696a998c85da2d4. It is best practice to apply a patch to resolve this issue.	3.1	More Details
CVE-2025-15416	A vulnerability was found in xnx3 wangmarket up to 6.4. This affects an unknown function of the file /siteVar/save.do of the component Add Global Variable Handler. The manipulation of the argument Remark/Variable Value results in cross site scripting. 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.	2.4	More Details
CVE-2025-15452	A weakness has been identified in xnx3 wangmarket up to 4.9. This affects the function variableList of the file /admin/system/variableList.do of the component Backend Variable Search. Executing a manipulation of the argument Description can lead to cross site scripting. 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.	2.4	More Details
CVE-2025-15372	A weakness has been identified in youlaitech vue3-element-admin up to 3.4.0. This issue affects some unknown processing of the file src/views/system/notice/index.vue of the component Notice Handler. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-15451	A security flaw has been discovered in xnx3 wangmarket up to 4.9. Affected by this issue is some unknown functionality of the file /admin/system/variableSave.do of the component System Variables Page. Performing a manipulation of the argument Description results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-11964	On Windows only, if libpcap needs to convert a Windows error message to UTF-8 and the message includes characters that UTF-8 represents using 4 bytes, utf_16le_to_utf_8_truncated() can write data beyond the end of the provided buffer.	1.9	More Details
	pcap_ether_aton() is an auxiliary function in libpcap, it takes a string argument and		

CVE-2025-11961	returns a fixed-size allocated buffer. The string argument must be a well-formed MAC-48 address in one of the supported formats, but this requirement has been poorly documented. If an application calls the function with an argument that deviates from the expected format, the function can read data beyond the end of the provided string and write data beyond the end of the allocated buffer.	1.9	More Details
CVE-2025-34584	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34969	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34524	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-66518	Any client who can access to Apache Kyuubi Server via Kyuubi frontend protocols can bypass server-side config kyuubi.session.local.dir.allow.list and use local files which are not listed in the config. This issue affects Apache Kyuubi: from 1.6.0 through 1.10.2. Users are recommended to upgrade to version 1.10.3 or upper, which fixes the issue.	N/A	More Details
CVE-2025-34507	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34505	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34498	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: s390/fpu: Fix false-positive kmsan report in fpu_vstl() A false-positive kmsan report is detected when running ping command. An inline assembly instruction 'vstl' can write varied amount of bytes depending on value of 'index' argument. If 'index' > 0, 'vstl' writes at least 2 bytes. clang generates kmsan write helper call depending on inline assembly constraints. Constraints are evaluated compile-time, but value of 'index' argument is known only at runtime. clang currently generates call to __msan_instrument_asm_store with 1 byte as size. Manually call kmsan function to indicate correct amount of bytes written and fix false-positive report. This change fixes following kmsan reports: [36.563119] == [36.563594] BUG: KMSAN: uninit-value in virtqueue_add+0x35c6/0x7c70 [36.563852] virtqueue_add+0x35c6/0x7c70 [36.564016] virtqueue_add_outbuf+0xa0/0xb0 [36.564266] start_xmit+0x288c/0x4a20 [36.564460] dev_hard_start_xmit+0x302/0x900 [36.564649] sch_direct_xmit+0x340/0xea0 [36.564894] __dev_queue_xmit+0x2e94/0x59b0 [36.565058] neigh_resolve_output+0x936/0xb40 [36.565278] __neigh_update+0x2f66/0x3a60 [36.565499] neigh_update+0x52/0x60 [36.565683] arp_process+0x1588/0x2de0 [36.565916] NF_HOOK+0x1da/0x240 [36.566087] arp_rcv+0x3e4/0x6e0 [36.566306] __netif_receive_skb_list_core+0x1374/0x15a0 [36.566527] netif_receive_skb_list_internal+0x1116/0x17d0 [36.566710] napi_complete_done+0x376/0x740 [36.566918] virtnet_poll+0x1bae/0x2910 [36.567130] __napi_poll+0xf4/0x830 [36.567294] net_rx_action+0x97c/0x1ed0 [36.567556] handle_softirqs+0x306/0xe10 [36.567731] irq_exit_rcu+0x14c/0x2e0 [36.567910] do_io_irq+0xd4/0x120 [36.568139] io_int_handler+0xc2/0xe8 [36.568299] arch_cpu_idle+0xb0/0xc0 [36.568540] arch_cpu_idle+0x76/0xc0 [36.568726]		

CVE-2025-68751	default_idle_call+0x40/0x70 [36.568953] do_idle+0x1d6/0x390 [36.569486] cpu_startup_entry+0x9a/0xb0 [36.569745] rest_init+0x1ea/0x290 [36.570029] start_kernel+0x95e/0xb90 [36.570348] startup_continue+0x2e/0x40 [36.570703] [36.570798] Uninit was created at: [36.571002] kmem_cache_alloc_node_noprof+0x9e8/0x10e0 [36.571261] kmalloc_reserve+0x12a/0x470 [36.571553] __alloc_skb+0x310/0x860 [36.571844] __ip_append_data+0x483e/0x6a30 [36.572170] ip_append_data+0x11c/0x1e0 [36.572477] raw_sendmsg+0x1c8c/0x2180 [36.572818] inet_sendmsg+0xe6/0x190 [36.573142] __sys_sendto+0x55e/0x8e0 [36.573392] __s390x_sys_socketcall+0x19ae/0x2ba0 [36.573571] __do_syscall+0x12e/0x240 [36.573823] system_call+0x6e/0x90 [36.573976] [36.574017] Byte 35 of 98 is uninitialized [36.574082] Memory access of size 98 starts at 0000000007aa0012 [36.574218] [36.574325] CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Tainted: G B N 6.17.0-dirty #16 NONE [36.574541] Tainted: [B]=BAD_PAGE, [N]=TEST [36.574617] Hardware name: IBM 3931 A01 703 (KVM/Linux) [36.574755] == [63.532541] == [63.533639] BUG: KMSAN: uninit-value in virtqueue_add+0x35c6/0x7c70 [63.533989] virtqueue_add+0x35c6/0x7c70 [63.534940] virtqueue_add_outbuf+0xa0/0xb0 [63.535861] start_xmit+0x288c/0x4a20 [63.536708] dev_hard_start_xmit+0x302/0x900 [63.537020] sch_direct_xmit+0x340/0xea0 [63.537997] __dev_queue_xmit+0x2e94/0x59b0 [63.538819] neigh_resolve_output+0x936/0xb40 [63.539793] ip_finish_output2+0x1ee2/0x2200 [63.540784] __ip_finish_output+0x272/0x7a0 [63.541765] ip_finish_output+0x4e/0x5e0 [63.542791] ip_output+0x166/0x410 [63.543771] ip_push_pending_frames+0x1a2/0x470 [63.544753] raw_sendmsg+0x1f06/0x2180 [63.545033] inet_sendmsg+0xe6/0x190 [63.546006] __sys_sendto+0x55e/0x8e0 ---truncated---	N/A	More Details
CVE-2025-68752	In the Linux kernel, the following vulnerability has been resolved: iavf: Implement settime64 with -EOPNOTSUPP ptp_clock_settime() assumes every ptp_clock has implemented settime64(). Stub it with -EOPNOTSUPP to prevent a NULL dereference. The fix is similar to commit 329d050bbe63 ("gve: Implement settime64 with -EOPNOTSUPP").	N/A	More Details
CVE-2025-68753	In the Linux kernel, the following vulnerability has been resolved: ALSA: firewire-motu: add bounds check in put_user loop for DSP events In the DSP event handling code, a put_user() loop copies event data. When the user buffer size is not aligned to 4 bytes, it could overwrite beyond the buffer boundary. Fix by adding a bounds check before put_user().	N/A	More Details
CVE-2025-68754	In the Linux kernel, the following vulnerability has been resolved: rtc: amlogic-a4: fix double free caused by devm The clock obtained via devm_clk_get_enabled() is automatically managed by devres and will be disabled and freed on driver detach. Manually calling clk_disable_unprepare() in error path and remove function causes double free. Remove the redundant clk_disable_unprepare() calls from the probe error path and aml_rtc_remove(), allowing the devm framework to automatically manage the clock lifecycle.	N/A	More Details
CVE-2025-68755	In the Linux kernel, the following vulnerability has been resolved: staging: most: remove broken i2c driver The MOST I2C driver has been completely broken for five years without anyone noticing so remove the driver from staging. Specifically, commit 723de0f9171e ("staging: most: remove device from interface structure") started requiring drivers to set the interface device pointer before registration, but the I2C driver was never updated which results in a NULL pointer dereference if anyone ever tries to probe it.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: block: Use RCU in blk_mq_[un]quiesce_tagset() instead of set->tag_list_lock		

CVE-2025-68756	blk_mq_{add,del}_queue_tag_set() functions add and remove queues from tagset, the functions make sure that tagset and queues are marked as shared when two or more queues are attached to the same tagset. Initially a tagset starts as unshared and when the number of added queues reaches two, blk_mq_add_queue_tag_set() marks it as shared along with all the queues attached to it. When the number of attached queues drops to 1 blk_mq_del_queue_tag_set() need to mark both the tagset and the remaining queues as unshared. Both functions need to freeze current queues in tagset before setting on unsetting BLK_MQ_F_TAG_QUEUE_SHARED flag. While doing so, both functions hold set->tag_list_lock mutex, which makes sense as we do not want queues to be added or deleted in the process. This used to work fine until commit 98d81f0df70c ("nvme: use blk_mq_[un]quiesce_tagset") made the nvme driver quiesce tagset instead of quiscing individual queues. blk_mq_quiesce_tagset() does the job and quiesce the queues in set->tag_list while holding set->tag_list_lock also. This results in deadlock between two threads with these stacktraces: __schedule+0x47c/0xbb0 ? timerqueue_add+0x66/0xb0 schedule+0x1c/0xa0 schedule_preempt_disabled+0xa/0x10 __mutex_lock.constprop.0+0x271/0x600 blk_mq_quiesce_tagset+0x25/0xc0 nvme_dev_disable+0x9c/0x250 nvme_timeout+0x1fc/0x520 blk_mq_handle_expired+0x5c/0x90 bt_iter+0x7e/0x90 blk_mq_queue_tag_busy_iter+0x27e/0x550 ? __blk_mq_complete_request_remote+0x10/0x10 ? __blk_mq_complete_request_remote+0x10/0x10 ? __call_rcu_common.constprop.0+0x1c0/0x210 blk_mq_timeout_work+0x12d/0x170 process_one_work+0x12e/0x2d0 worker_thread+0x288/0x3a0 ? rescuer_thread+0x480/0x480 kthread+0xb8/0xe0 ? kthread_park+0x80/0x80 ret_from_fork+0x2d/0x50 ? kthread_park+0x80/0x80 ret_from_fork_asm+0x11/0x20 __schedule+0x47c/0xbb0 ? xas_find+0x161/0x1a0 schedule+0x1c/0xa0 blk_mq_freeze_queue_wait+0x3d/0x70 ? destroy_sched_domains_rcu+0x30/0x30 blk_mq_update_tag_set_shared+0x44/0x80 blk_mq_exit_queue+0x141/0x150 del_gendisk+0x25a/0x2d0 nvme_ns_remove+0xc9/0x170 nvme_remove_namespaces+0xc7/0x100 nvme_remove+0x62/0x150 pci_device_remove+0x23/0x60 device_release_driver_internal+0x159/0x200 unbind_store+0x99/0xa0 kernfs_fop_write_iter+0x112/0x1e0 vfs_write+0x2b1/0x3d0 ksys_write+0x4e/0xb0 do_syscall_64+0x5b/0x160 entry_SYSCALL_64_after_hwframe+0x4b/0x53 The top stacktrace is showing nvme_timeout() called to handle nvme command timeout. timeout handler is trying to disable the controller and as a first step, it needs to blk_mq_quiesce_tagset() to tell blk-mq not to call queue callback handlers. The thread is stuck waiting for set->tag_list_lock as it tries to walk the queues in set->tag_list. The lock is held by the second thread in the bottom stack which is waiting for one of queues to be frozen. The queue usage counter will drop to zero after nvme_timeout() finishes, and this will not happen because the thread will wait for this mutex forever. Given that [un]quiescing queue is an operation that does not need to sleep, update blk_mq_[un]quiesce_tagset() to use RCU instead of taking set->tag_list_lock, update blk_mq_{add,del}_queue_tag_set() to use RCU safe list operations. Also, delete INIT_LIST_HEAD(&q->tag_set_list) in blk_mq_del_queue_tag_set() because we can not re-initialize it while the list is being traversed under RCU. The deleted queue will not be added/deleted to/from a tagset and it will be freed in blk_free_queue() after the end of RCU grace period.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/vgem-fence: Fix potential deadlock on release A timer that expires a vgem fence automatically in 10 seconds is now released with timer_delete_sync() from fence->ops.release() called on last dma_fence_put(). In some scenarios, it can run in IRQ context, which is not safe unless TIMER_IRQSAFE is used. One potentially risky scenario was demonstrated in Intel DRM CI trybot, BAT run on machine bat-adlp-6, while working on new IGT subtests syncobj_timeline@stress-* as user space replacements of some problematic test cases of a dma-fence-chain selftest [1]. [117.004338] ================================ [117.004340] WARNING: inconsistent lock state [117.004342] 6.17.0-rc7-CI_DRM_17270-g7644974e648c+ #1 Tainted: G S U [117.004346] -------------------------------- [117.004347] inconsistent		

CVE-2025-68757	{HARDIRQ-ON-W} -> {IN-HARDIRQ-W} usage. [117.004349] swapper/0/0 [HC1[1]:SC1[1]:HE0:SE0] takes: [117.004352] ffff888138f86aa8 ((&fence->timer)){?.-.}-{0:0}, at: __timer_delete_sync+0x4b/0x190 [117.004361] {HARDIRQ-ON-W} state was registered at: [117.004363] lock_acquire+0xc4/0x2e0 [117.004366] call_timer_fn+0x80/0x2a0 [117.004368] __run_timers+0x231/0x310 [117.004370] run_timer_softirq+0x76/0xe0 [117.004372] handle_softirqs+0xd4/0x4d0 [117.004375] __irq_exit_rcu+0x13f/0x160 [117.004377] irq_exit_rcu+0xe/0x20 [117.004379] sysvec_apic_timer_interrupt+0xa0/0xc0 [117.004382] asm_sysvec_apic_timer_interrupt+0x1b/0x20 [117.004385] cpuidle_enter_state+0x12b/0x8a0 [117.004388] cpuidle_enter+0x2e/0x50 [117.004393] call_cpuidle+0x22/0x60 [117.004395] do_idle+0x1fd/0x260 [117.004398] cpu_startup_entry+0x29/0x30 [117.004401] start_secondary+0x12d/0x160 [117.004404] common_startup_64+0x13e/0x141 [117.004407] irq event stamp: 2282669 [117.004409] hardirqs last enabled at (2282668): [<ffffffff8289db71>] _raw_spin_unlock_irqrestore+0x51/0x80 [117.004414] hardirqs last disabled at (2282669): [<ffffffff82882021>] sysvec_irq_work+0x11/0xc0 [117.004419] softirqs last enabled at (2254702): [<ffffffff8289fd00>] __do_softirq+0x10/0x18 [117.004423] softirqs last disabled at (2254725): [<ffffffff813d4ddf>] __irq_exit_rcu+0x13f/0x160 [117.004426] other info that might help us debug this: [117.004429] Possible unsafe locking scenario: [117.004432] CPU0 [117.004433] ---- [117.004434] lock((&fence->timer)); [117.004436] <Interrupt> [117.004438] lock((&fence->timer)); [117.004440] *** DEADLOCK *** [117.004443] 1 lock held by swapper/0/0: [117.004445] #0: ffffc90000003d50 ((&fence->timer)){?.-.}-{0:0}, at: call_timer_fn+0x7a/0x2a0 [117.004450] stack backtrace: [117.004453] CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Tainted: G S U 6.17.0-rc7-CI_DRM_17270-g7644974e648c+ #1 PREEMPT(voluntary) [117.004455] Tainted: [S]=CPU_OUT_OF_SPEC, [U]=USER [117.004455] Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-P DDR4 RVP, BIOS RPLPFWI1.R00.4035.A00.2301200723 01/20/2023 [117.004456] Call Trace: [117.004456] <IRQ> [117.004457] dump_stack_lvl+0x91/0xf0 [117.004460] dump_stack+0x10/0x20 [117.004461] print_usage_bug.part.0+0x260/0x360 [117.004463] mark_lock+0x76e/0x9c0 [117.004465] ? register_lock_class+0x48/0x4a0 [117.004467] __lock_acquire+0xbc3/0x2860 [117.004469] lock_acquire+0xc4/0x2e0 [117.004470] ? __timer_delete_sync+0x4b/0x190 [117.004472] ? __timer_delete_sync+0x4b/0x190 [117.004473] __timer_delete_sync+0x68/0x190 [117.004474] ? __timer_delete_sync+0x4b/0x190 [117.004475] timer_delete_sync+0x10/0x20 [117.004476] vgem_fence_release+0x19/0x30 [vgem] [117.004478] dma_fence_release+0xc1/0x3b0 [117.004480] ? dma_fence_release+0xa1/0x3b0 [117.004481] dma_fence_chain_release+0xe7/0x130 [117.004483] dma_fence_release+0xc1/0x3b0 [117.004484] ? _raw_spin_unlock_irqrestore+0x27/0x80 [117.004485] dma_fence_chain_irq_work+0x59/0x80 [117.004487] irq_work_single+0x75/0xa0 [117.004490] irq_work_r ---truncated---	N/A	More Details
CVE-2025-68758	In the Linux kernel, the following vulnerability has been resolved: backlight: led-bl: Add devlink to supplier LEDs LED Backlight is a consumer of one or multiple LED class devices, but devlink is currently unable to create correct supplier-producer links when the supplier is a class device. It creates instead a link where the supplier is the parent of the expected device. One consequence is that removal order is not correctly enforced. Issues happen for example with the following sections in a device tree overlay: // An LED driver chip pca9632@62 { compatible = "nxp,pca9632"; reg = <0x62>; // ... addon_led_pwm: led-pwm@3 { reg = <3>; label = "addon:led:pwm"; }; }; backlight-addon { compatible = "led-backlight"; leds = <&addon_led_pwm>; brightness-levels = <255>; default-brightness-level = <255>; }; In this example, the devlink should be created between the backlight-addon (consumer) and the pca9632@62 (supplier). Instead it is created between the backlight-addon (consumer) and the parent of the pca9632@62, which is typically the I2C bus adapter. On removal of the above overlay, the LED driver can be removed before the backlight device, resulting in: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010 ... Call trace: led_put+0xe0/0x140 devm_led_release+0x6c/0x98	N/A	More Details

	Another way to reproduce the bug without any device tree overlays is unbinding the LED class device (pca9632@62) before unbinding the consumer (backlight-addon): echo 11-0062 >/sys/bus/i2c/drivers/leds-pca963x/unbind echo ...backlight-dock >/sys/bus/platform/drivers/led-backlight/unbind Fix by adding a devlink between the consuming led-backlight device and the supplying LED device, as other drivers and subsystems do as well.		
CVE-2025-68759	In the Linux kernel, the following vulnerability has been resolved: wifi: rtl818x: Fix potential memory leaks in rtl8180_init_rx_ring() In rtl8180_init_rx_ring(), memory is allocated for skb packets and DMA allocations in a loop. When an allocation fails, the previously successful allocations are not freed on exit. Fix that by jumping to err_free_rings label on error, which calls rtl8180_free_rx_ring() to free the allocations. Remove the free of rx_ring in rtl8180_init_rx_ring() error path, and set the freed priv->rx_buf entry to null, to avoid double free.	N/A	More Details
CVE-2025-68760	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Fix potential out-of-bounds read in iommu_mmio_show In iommu_mmio_write(), it validates the user-provided offset with the check: `iommu->dbg_mmio_offset > iommu->mmio_phys_end - 4`. This assumes a 4-byte access. However, the corresponding show handler, iommu_mmio_show(), uses readq() to perform an 8-byte (64-bit) read. If a user provides an offset equal to `mmio_phys_end - 4`, the check passes, and will lead to a 4-byte out-of-bounds read. Fix this by adjusting the boundary check to use sizeof(u64), which corresponds to the size of the readq() operation.	N/A	More Details
CVE-2025-68761	In the Linux kernel, the following vulnerability has been resolved: hfs: fix potential use after free in hfs_correct_next_unused_CNID() This code calls hfs_bnode_put(node) which drops the refcount and then dreferences "node" on the next line. It's only safe to use "node" when we're holding a reference so flip these two lines around.	N/A	More Details
CVE-2025-68762	In the Linux kernel, the following vulnerability has been resolved: net: netpoll: initialize work queue before error checks Prevent a kernel warning when netconsole setup fails on devices with IFF_DISABLE_NETPOLL flag. The warning (at kernel/workqueue.c:4242 in __flush_work) occurs because the cleanup path tries to cancel an uninitialized work queue. When __netpoll_setup() encounters a device with IFF_DISABLE_NETPOLL, it fails early and calls skb_pool_flush() for cleanup. This function calls cancel_work_sync(&np->refill_wq), but refill_wq hasn't been initialized yet, triggering the warning. Move INIT_WORK() to the beginning of __netpoll_setup(), ensuring the work queue is properly initialized before any potential failure points. This allows the cleanup path to safely cancel the work queue regardless of where the setup fails.	N/A	More Details
CVE-2025-68763	In the Linux kernel, the following vulnerability has been resolved: crypto: starfive - Correctly handle return of sg_nents_for_len The return value of sg_nents_for_len was assigned to an unsigned long in starfive_hash_digest, causing negative error codes to be converted to large positive integers. Add error checking for sg_nents_for_len and return immediately on failure to prevent potential buffer overflows.	N/A	More Details
CVE-2025-68764	In the Linux kernel, the following vulnerability has been resolved: NFS: Automounted filesystems should inherit ro,noexec,nodev,sync flags When a filesystem is being automounted, it needs to preserve the user-set superblock mount options, such as the "ro" flag.	N/A	More Details
CVE-2025-68765	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7615: Fix memory leak in mt7615_mcu_wtbl_sta_add() In mt7615_mcu_wtbl_sta_add(), an skb sskb is allocated. If the subsequent call to mt76_connac_mcu_alloc_wtbl_req() fails, the function returns an error without freeing sskb, leading to a memory leak. Fix this by calling dev_kfree_skb() on sskb in the error handling path to ensure it is properly released.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: irqchip/mchp-eic: Fix error code in mchp_eic_domain_alloc() If irq_domain_translate_twocell() sets "hwirq" to >= MCHP_EIC_NIRQ (2) then it results in an out of bounds access. The code checks for	N/A	More Details

68766	invalid values, but doesn't set the error code. Return -EINVAL in that case, instead of returning success.		
CVE-2025-34525	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34526	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34527	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34538	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34546	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-5591	Kentico Xperience 13 is vulnerable to a stored cross-site scripting attack via a form component, allowing an attacker to hijack a victim user’s session and perform actions in their security context.	N/A	More Details
CVE-2025-34545	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34544	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34543	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34542	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34541	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34540	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34539	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34537	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34528	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34536	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34535	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34534	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34533	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34532	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34531	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-15022	Action captions in Vaadin accept HTML by default but were not sanitized, potentially allowing Cross-site Scripting (XSS) if caption content is derived from user input. In Vaadin Framework 7 and 8, the Action class is a general-purpose class that may be used by multiple components. The fixed versions sanitize captions by default and provide an API to explicitly enable HTML content mode for backwards compatibility. In Vaadin 23 and newer, the Action class is only used by the Spreadsheet component. The fixed versions sanitize HTML using Jsoup with a relaxed safelist. Vaadin 14 is not affected as Spreadsheet component was not supported. Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include: Product version Vaadin 7.0.0 - 7.7.49 Vaadin 8.0.0 - 8.29.1 Vaadin 23.1.0 - 23.6.5 Vaadin 24.0.0 - 24.8.13 Vaadin 24.9.0 - 24.9.6 Mitigation Upgrade to 7.7.50 Upgrade to 8.30.0 Upgrade to 23.6.6 Upgrade to 24.8.14 or 24.9.7 Upgrade to 25.0.0 or newer Artifacts Maven coordinatesVulnerable versionsFixed versioncom.vaadin:vaadin-server 7.0.0 - 7.7.49 ≥7.7.50 com.vaadin:vaadin-server 8.0.0 - 8.29.1 ≥8.30.0 com.vaadin:vaadin 23.1.0 - 23.6.5 ≥23.6.6 com.vaadin:vaadin24.0.0 - 24.8.13 ≥24.8.14 com.vaadin:vaadin24.9.0 - 24.9.6 ≥24.9.7 com.vaadin:vaadin-spreadsheet-flow 23.1.0 - 23.6.5 ≥23.6.6 com.vaadin:vaadin-spreadsheet-flow 24.0.0 - 24.8.13 ≥24.8.14 com.vaadin:vaadin-spreadsheet-flow 24.9.0 - 24.9.6 ≥24.9.7	N/A	More Details
CVE-2025-34530	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34529	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34497	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34496	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34495			
CVE-2025-10933	An integer underflow vulnerability in the Silicon Labs Z-Wave Protocol Controller can lead to out of bounds memory reads.	N/A	More Details
CVE-2025-34463	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34462	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34461	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34460	Rejected reason: This candidate has been reserved by a CVE Numbering Authority (CNA).	N/A	More Details
CVE-2025-34459	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34456	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34455	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34454	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34453	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34448	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34465	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34447	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34446	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34445	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34444	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34443	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34432	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34431	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34426	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34415	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34464	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34466	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34494	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34481	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34493	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34492	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34488	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34487	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34486	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34485	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34484	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34483	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34482	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34480	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34470	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34479	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34478	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34477	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34476	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34475	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34474	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34473	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34472	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34471	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34547	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a	N/A	More

34548	vulnerability disclosure.		Details
CVE-2025-34549	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34581	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34995	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34996	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34997	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34998	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34999	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-35000	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-35001	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-35002	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34582	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34580	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34993	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34579	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34578	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34577	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34576	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34575	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34574	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34573	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21429	Emlog is an open source website building system. In version 2.5.23, the admin can set controls which makes users unable to edit or delete their articles after publishing them. As of time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-34572	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34994	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34992	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21430	Emlog is an open source website building system. In version 2.5.23, article creation functionality is vulnerable to cross-site request forgery (CSRF). This can lead to a user being forced to post an article with arbitrary, attacker-controlled content. This, when combined with stored cross-site scripting, leads to account takeover. As of time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-34980	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34971	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34972	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34973	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34974	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34975	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34976	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34977	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34978	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34979	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34981	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34991	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34982	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34983	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34984	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34985	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34986	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34987	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34988	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34989	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34990	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34571	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21431	Emlog is an open source website building system. Version 2.5.23 has a stored cross-site scripting vulnerability in the `Resource media library ` function while publishing an article. As of time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-34550	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34561	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21647	Rejected reason: Not used	N/A	More Details
CVE-2026-21648	Rejected reason: Not used	N/A	More Details
CVE-2026-21649	Rejected reason: Not used	N/A	More Details
CVE-2026-21650	Rejected reason: Not used	N/A	More Details
CVE-2026-21651	Rejected reason: Not used	N/A	More Details
CVE-2026-21652	Rejected reason: Not used	N/A	More Details
CVE-2025-34564	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34563	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34562	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34560	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21645	Rejected reason: Not used	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34559			
CVE-2025-34558	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34557	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34556	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34555	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34554	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34553	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34552	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34551	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21646	Rejected reason: Not used	N/A	More Details
CVE-2026-21644	Rejected reason: Not used	N/A	More Details
CVE-2026-21432	Emlog is an open source website building system. Version 2.5.23 has a stored cross-site scripting vulnerability that can lead to account takeover, including takeover of admin accounts. As of time of publication, no known patched versions are available.	N/A	More Details
CVE-2026-21450	Bagisto is an open source laravel eCommerce platform. Versions prior to 2.3.10 are vulnerable to server-side template injection via type parameter, which can lead to remote code execution or another exploitation. Version 2.3.10 fixes the issue.	N/A	More Details
CVE-2025-34570	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21440	AdonisJS is a TypeScript-first web framework. A Path Traversal vulnerability in AdonisJS multipart file handling may allow a remote attacker to write arbitrary files to arbitrary locations on the server filesystem. This impacts @adonisjs/bodyparser through version 10.1.1 and 11.x prerelease versions prior to 11.0.0-next.6. This issue has been patched in @adonisjs/bodyparser versions 10.1.2 and 11.0.0-next.6.	N/A	More Details
CVE-2025-34569	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34568	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21445	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.7.0.dev45, multiple critical API endpoints in Langflow are missing authentication controls. The issue allows any unauthenticated user to access sensitive user conversation data, transaction histories, and perform destructive operations including message deletion. This affects endpoints handling personal data and system operations that should require proper authorization. Version 1.7.0.dev45 contains a patch.	N/A	More Details
CVE-2026-21446	Bagisto is an open source laravel eCommerce platform. In versions on the 2.3 branch prior to 2.3.10, API routes remain active even after initial installation is complete. The underlying API endpoints (`/install/api/*`) are directly accessible and exploitable without any authentication. An attacker can bypass the Ib installer entirely by calling the API endpoints directly. This allows any unauthenticated attacker to create admin accounts, modify application configurations, and potentially overwrite existing data. Version 2.3.10 fixes the issue.	N/A	More Details
CVE-2025-34567	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21448	Bagisto is an open source laravel eCommerce platform. Versions prior to 2.3.10 are vulnerable to server-side template injection. When a normal customer orders any product, in the `add address` step they can inject a value to run in admin view. The issue can lead to remote code execution. Version 2.3.10 contains a patch.	N/A	More Details
CVE-2026-21449	Bagisto is an open source laravel eCommerce platform. Versions prior to 2.3.10 are vulnerable to server-side template injection via first name and last name from a low-privilege user. Version 2.3.10 fixes the issue.	N/A	More Details
CVE-2026-21451	Bagisto is an open source laravel eCommerce platform. A stored Cross-Site Scripting (XSS) vulnerability exists in Bagisto prior to version 2.3.10 within the CMS page editor. Although the platform normally attempts to sanitize `<script>` tags, the filtering can be bypassed by manipulating the raw HTTP POST request before submission. As a result, arbitrary JavaScript can be stored in the CMS content and executed whenever the page is viewed or edited. This exposes administrators to a high-severity risk, including complete account takeover, backend hijacking, and malicious script execution. Version 2.3.10 fixes the issue.	N/A	More Details
CVE-2025-34565	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34566	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21483	listmonk is a standalone, self-hosted, newsletter and mailing list manager. Prior to version 6.0.0, lower-privileged user with campaign management permissions can inject malicious JavaScript into campaigns or templates. When a higher-privileged user (Super Admin) views or previews this content, the XSS executes in their browser context, allowing the attacker to perform privileged actions such as creating backdoor admin accounts. The attack can be weaponized via the public archive feature, where victims simply need to visit a link - no preview click required. Version 6.0.0 fixes the issue.	N/A	More Details
CVE-2025-	A vulnerability in Nuvation Battery Management System allows Authentication Bypass.This issue affects Battery Management System: through 2.3.9.	N/A	More Details

64119			
CVE-2025-64120	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows OS Command Injection.This issue affects Multi-Stack Controller (MSC): from 2.3.8 before 2.5.1.	N/A	More Details
CVE-2025-64121	Authentication Bypass Using an Alternate Path or Channel vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows Authentication Bypass.This issue affects Multi-Stack Controller (MSC): from 2.3.8 before 2.5.1.	N/A	More Details
CVE-2025-64122	Insufficiently Protected Credentials vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows Signature Spoofing by Key Theft.This issue affects Multi-Stack Controller (MSC): through 2.5.1.	N/A	More Details
CVE-2025-64123	Unintended Proxy or Intermediary vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows Network Boundary Bridging.This issue affects Multi-Stack Controller (MSC): through and including release 2.5.1.	N/A	More Details
CVE-2025-64124	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows OS Command Injection.This issue affects Multi-Stack Controller (MSC): before 2.5.1.	N/A	More Details
CVE-2025-64125	A vulnerability in Nuvation Energy nCloud VPN Service allowed Network Boundary Bridging.This issue affected the nCloud VPN Service and was fixed on 2025-12-1 (December, 2025). End users do not have to take any action to mitigate the issue.	N/A	More Details
CVE-2025-34405	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34391	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-59156	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.420.7, a Remote Code Execution (RCE)*vulnerability exists in Coolify's application deployment workflow. This flaw allows a low-privileged member to inject arbitrary Docker Compose directives during project creation or updates. By defining a malicious service that mounts the host filesystem, an attacker can achieve root-level command execution on the host OS, completely bypassing container isolation. Version 4.0.0-beta.420.7 contains a patch for the issue.	N/A	More Details
CVE-2025-22202	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-59387	An SQL injection vulnerability has been reported to affect MARS (Multi-Application Recovery Service). The remote attackers can then exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following version: MARS (Multi-Application Recovery Service) 1.2.1.1686 and later	N/A	More Details
CVE-2025-59384	A path traversal vulnerability has been reported to affect Qfiling. The remote attackers can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: Qfiling 3.13.1 and later	N/A	More Details
CVE-2025-53594	A path traversal vulnerability has been reported to affect several product versions. If a local attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following versions: Qfinder Pro Mac 7.13.0 and later Qsync for Mac 5.1.5 and later QVPN Device Client for Mac 2.2.8 and later	N/A	More Details

CVE-2025-11837	An improper control of generation of code vulnerability has been reported to affect Malware Remover. The remote attackers can then exploit the vulnerability to bypass protection mechanism. We have already fixed the vulnerability in the following version: Malware Remover 6.6.8.20251023 and later	N/A	More Details
CVE-2026-21437	eopkg is a Solus package manager implemented in python3. In versions prior to 4.4.0, a malicious package could include files that are not tracked by `eopkg`. This requires the installation of a package from a malicious or compromised source. Files in such packages would not be shown by `lseopkg` and related tools. The issue has been fixed in v4.4.0. Users only installing packages from the Solus repositories are not affected.	N/A	More Details
CVE-2026-21436	eopkg is a Solus package manager implemented in python3. In versions prior to 4.4.0, a malicious package could escape the directory set by `--destdir`. This requires the installation of a package from a malicious or compromised source. Files in such packages would not be installed in the path given by `--destdir`, but on a different location on the host. The issue has been fixed in v4.4.0. Users only installing packages from the Solus repositories are not affected.	N/A	More Details
CVE-2025-66023	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Versions prior to 0.24.5 have a Heap-Use-After-Free (UAF) vulnerability within the MQTT bridge client component (implemented via the underlying NanoNNG library). The vulnerability is triggered when NanoMQ acts as a bridge connecting to a remote MQTT broker. A malicious remote broker can trigger a crash (Denial of Service) or potential memory corruption by accepting the connection and immediately sending a malformed packet sequence. Version 0.34.5 contains a patch. The patch enforces stricter protocol adherence in the MQTT client SDK embedded in NanoMQ. Specifically, it ensures that CONNACK is always the first packet processed in the line. This prevents the state confusion that led to the Heap-Use-After-Free (UAF) when a malicious server sent a malformed packet sequence immediately after connection establishment. As a workaround, validate the remote broker before bridging.	N/A	More Details
CVE-2025-11157	A high-severity remote code execution vulnerability exists in feast-dev/feast version 0.53.0, specifically in the Kubernetes materializer job located at `feast/sdk/python/feast/infra/compute_engines/kubernetes/main.py`. The vulnerability arises from the use of `yaml.load(..., Loader=yaml.Loader)` to deserialize `/var/feast/feature_store.yaml` and `/var/feast/materialization_config.yaml`. This method allows for the instantiation of arbitrary Python objects, enabling an attacker with the ability to modify these YAML files to execute OS commands on the worker pod. This vulnerability can be exploited before the configuration is validated, potentially leading to cluster takeover, data poisoning, and supply-chain sabotage.	N/A	More Details
CVE-2025-22203	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22201	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-62840	A generation of error message containing sensitive information vulnerability has been reported to affect HBS 3 Hybrid Backup Sync. If an attacker gains local network access, they can then exploit the vulnerability to read application data. We have already fixed the vulnerability in the following version: HBS 3 Hybrid Backup Sync 26.2.0.938 and later	N/A	More Details
CVE-2025-22200	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details

22199			
CVE-2025-22198	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22197	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22196	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22195	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22194	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-14979	AirVPN Eddie on MacOS contains an insecure XPC service that allows local, unprivileged users to escalate their privileges to root.This issue affects Eddie: 2.24.6.	N/A	More Details
CVE-2025-22193	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-59389	An SQL injection vulnerability has been reported to affect Hyper Data Protector. The remote attackers can then exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following versions: Hyper Data Protector 2.2.4.1 and later	N/A	More Details
CVE-2025-62842	An external control of file name or path vulnerability has been reported to affect HBS 3 Hybrid Backup Sync. If an attacker gains local network access, they can then exploit the vulnerability to read or modify files or directories. We have already fixed the vulnerability in the following version: HBS 3 Hybrid Backup Sync 26.2.0.938 and later	N/A	More Details
CVE-2025-22191	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-34170	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-21747	Rejected reason: Not used	N/A	More Details
CVE-2026-21748	Rejected reason: Not used	N/A	More Details
CVE-2026-21749	Rejected reason: Not used	N/A	More Details
CVE-2026-	Rejected reason: Not used	N/A	More Details

21750			
CVE-2025-34250	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34219	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34214	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34213	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34171	CasaOS versions up to and including 0.4.15 expose multiple unauthenticated endpoints that allow remote attackers to retrieve sensitive configuration files and system debug information. The /v1/users/image endpoint can be abused with a user-controlled path parameter to access files under /var/lib/casaos/1/, which reveals installed applications and configuration details. Additionally, /v1/sys/debug discloses host operating system, kernel, hardware, and storage information. The endpoints also return distinct error messages, enabling file existence enumeration of arbitrary paths on the underlying host filesystem. This information disclosure can be used for reconnaissance and to facilitate targeted follow-up attacks against services deployed on the host.	N/A	More Details
CVE-2026-21411	Authentication bypass issue exists in OpenBlocks series versions prior to FW5.0.8, which may allow an attacker to bypass administrator authentication and change the password.	N/A	More Details
CVE-2025-34094	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34169	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34168	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34167	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34166	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34145	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34144	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34137	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34131	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34122	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-22192	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22190	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2026-21745	Rejected reason: Not used	N/A	More Details
CVE-2025-15382	A heap buffer over-read vulnerability exists in the wolfSSH_CleanPath() function in wolfSSH. An authenticated remote attacker can trigger the issue via crafted SCP path input containing '/./' sequences, resulting in a heap over read by 1 byte.	N/A	More Details
CVE-2025-69356	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) thegem-elements-elementor allows PHP Local File Inclusion.This issue affects TheGem Theme Elements (for Elementor): from n/a through <= 5.11.0.	N/A	More Details
CVE-2025-15279	FontForge GUtils BMP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 pixels within BMP 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 user. Was ZDI-CAN-27517.	N/A	More Details
CVE-2025-69359	Missing Authorization vulnerability in WPFunnels Creator LMS creatorlms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Creator LMS: from n/a through <= 1.1.12.	N/A	More Details
CVE-2025-15278	FontForge GUtils XBM File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 pixels within XBM files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27865.	N/A	More Details
CVE-2025-69361	Missing Authorization vulnerability in PublishPress Post Expirator post-expirator allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post Expirator: from n/a through <= 4.9.3.	N/A	More Details
CVE-2025-15277	FontForge GUtils SGI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 scanlines within SGI files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it	N/A	More Details

	to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27920.		
CVE-2025-69363	Missing Authorization vulnerability in CyberChimps Responsive Addons for Elementor responsive-addons-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Responsive Addons for Elementor: from n/a through <= 2.0.8.	N/A	More Details
CVE-2025-69364	Missing Authorization vulnerability in Cloudways Breeze breeze allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Breeze: from n/a through <= 2.2.21.	N/A	More Details
CVE-2025-14942	wolfSSH’s key exchange state machine can be manipulated to leak the client’s password in the clear, trick the client to send a bogus signature, or trick the client into skipping user authentication. This affects client applications with wolfSSH version 1.4.21 and earlier. Users of wolfSSH must update or apply the fix patch and it’s recommended to update credentials used. This fix is also recommended for wolfSSH server applications. While there aren’t any specific attacks on server applications, the same defect is present. Thanks to Aina Toky Rasoamanana of Valeo and Olivier Levillain of Telecom SudParis for the report.	N/A	More Details
CVE-2025-15276	FontForge SFD File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD files. 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 the current process. Was ZDI-CAN-28198.	N/A	More Details
CVE-2025-15280	FontForge SFD File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28525.	N/A	More Details
CVE-2025-15275	FontForge SFD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD 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 user. Was ZDI-CAN-28543.	N/A	More Details
CVE-2025-15274	FontForge SFD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD 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 user. Was ZDI-CAN-28544.	N/A	More Details
CVE-2025-15273	FontForge PFB File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 PFB files. The issue results from the lack of	N/A	More Details

	proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28546.		
CVE-2025-15272	FontForge SFD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD 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 user. Was ZDI-CAN-28547.	N/A	More Details
CVE-2023-5069	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-15271	FontForge SFD File Parsing Improper Validation of Array Index Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD 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 array. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28562.	N/A	More Details
CVE-2025-13744	An Improper Neutralization of Input During Web Page Generation vulnerability was identified in GitHub Enterprise Server that allowed attacker controlled HTML to be rendered by the Filter component (search) across GitHub that could be used to exfiltrate sensitive information. An attacker would require permissions to create or modify the names of milestones, issues, pull requests, or similar entities that are rendered in the vulnerable filter/search components. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.20 and was fixed in versions 3.19.1, and 3.18.2, 3.17.8, 3.16.11, 3.15.15, and 3.14.20. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2025-15270	FontForge SFD File Parsing Improper Validation of Array Index Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD 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 array. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28563.	N/A	More Details
CVE-2025-15269	FontForge SFD File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of FontForge. 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 SFD files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28564.	N/A	More Details
CVE-2025-69355	Missing Authorization vulnerability in Tickera Tickera tickera-event-ticketing-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tickera: from n/a through <= 3.5.6.4.	N/A	More Details
CVE-2025-	A vulnerability exists in serial device servers where active debug code remains enabled in the UART interface. An attacker with physical access to the device can directly connect to the UART interface and, without authentication, user interaction, or execution conditions, gain unauthorized access to internal debug functionality.	N/A	More

15017	Exploitation is low complexity and allows an attacker to execute privileged operations and access sensitive system resources, resulting in a high impact to the confidentiality, integrity, and availability of the affected device. No security impact to external or dependent systems has been identified.		Details
CVE-2025-22189	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22181	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22188	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-63082	Lack of input filtering leads to an XSS vector in the HTML filter code related to data URLs in img tags.	N/A	More Details
CVE-2025-63083	Lack of output escaping leads to a XSS vector in the pagebreak plugin.	N/A	More Details
CVE-2025-22187	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22186	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22185	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22184	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22183	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22182	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-69335	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Team Showcase team-showcase allows Stored XSS.This issue affects Team Showcase: from n/a through <= 2.9.	N/A	More Details
CVE-2025-1977	The NPort 6100-G2/6200-G2 Series is affected by an execution with unnecessary privileges vulnerability (CVE-2025-1977) that allows an authenticated user with read-only access to perform unauthorized configuration changes through the MCC (Moxa CLI Configuration) tool. The issue can be exploited remotely over the network with low-attack complexity and no user interaction but requires specific system conditions or configurations to be present. Successful exploitation may result in changes to device settings that were not intended to be permitted for the affected user role, potentially leading to a high impact on the confidentiality, integrity, and availability of the device. No impact on other systems has been identified.	N/A	More Details

CVE-2025-22180	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22155	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-22154	Rejected reason: To maintain compliance with CNA rules, we have rejected this CVE record because it has not been used.	N/A	More Details
CVE-2025-34469	Cowrie versions prior to 2.9.0 contain a server-side request forgery (SSRF) vulnerability in the emulated shell implementation of wget and curl. In the default emulated shell configuration, these command emulations perform real outbound HTTP requests to attacker-supplied destinations. Because no outbound request rate limiting was enforced, unauthenticated remote attackers could repeatedly invoke these commands to generate unbounded HTTP traffic toward arbitrary third-party targets, allowing the Cowrie honeypot to be abused as a denial-of-service amplification node and masking the attacker’s true source address behind the honeypot’s IP.	N/A	More Details
CVE-2023-7332	PocketMine-MP versions prior to 4.18.1 contain an improper input validation vulnerability in inventory transaction handling. A remote attacker with a valid player session can request that the server drop more items than are available in the player's hotbar, triggering a server crash and resulting in denial of service.	N/A	More Details
CVE-2015-10145	Gargoyle router management utility versions 1.5.x contain an authenticated OS command execution vulnerability in /utility/run_commands.sh. The application fails to properly restrict or validate input supplied via the 'commands' parameter, allowing an authenticated attacker to execute arbitrary shell commands on the underlying system. Successful exploitation may result in full compromise of the device, including unauthorized access to system files and execution of attacker-controlled commands.	N/A	More Details
CVE-2025-34468	libcoap versions up to and including 4.3.5, prior to commit 30db3ea, contain a stack-based buffer overflow in address resolution when attacker-controlled hostname data is copied into a fixed 256-byte stack buffer without proper bounds checking. A remote attacker can trigger a crash and potentially achieve remote code execution depending on compiler options and runtime memory protections. Exploitation requires the proxy logic to be enabled (i.e., the proxy request handling code path in an application using libcoap).	N/A	More Details
CVE-2025-34467	ZwiiCMS versions prior to 13.7.00 contain a denial-of-service vulnerability in multiple administrative endpoints due to improper authorization checks combined with flawed resource state management. When an authenticated low-privilege user requests an administrative page, the application returns "404 Not Found" as expected, but incorrectly acquires and associates a temporary lock on the targeted resource with the attacker session prior to authorization. This lock prevents other users, including administrators, from accessing the affected functionality until the attacker navigates away or the session is terminated.	N/A	More Details
CVE-2025-2026	The NPort 6100-G2/6200-G2 Series is affected by a high-severity vulnerability (CVE-2025-2026) that allows remote attackers to execute a null byte injection through the device’s web API. This may lead to an unexpected device reboot and result in a denial-of-service (DoS) condition. An authenticated remote attacker with web read-only privileges can exploit the vulnerable API to inject malicious input. Successful exploitation may cause the device to reboot, disrupting normal operations and causing a temporary denial of service.	N/A	More Details
CVE-2026-21746	Rejected reason: Not used	N/A	More Details

CVE-2026-21744	Rejected reason: Not used	N/A	More Details
CVE-2025-59158	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Coolify versions prior to and including v4.0.0-beta.420.6 are vulnerable to a stored cross-site scripting (XSS) attack in the project creation workflow. An authenticated user with low privileges (e.g., member role) can create a project with a maliciously crafted name containing embedded JavaScript. When an administrator later attempts to delete the project or its associated resource, the payload automatically executes in the admin's browser context. Version 4.0.0-beta.420.7 contains a patch for the issue.	N/A	More Details
CVE-2025-34376	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34378	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-67732	Dify is an open-source LLM app development platform. Prior to version 1.11.0, the API key is exposed in plaintext to the frontend, allowing non-administrator users to view and reuse it. This can lead to unauthorized access to third-party services, potentially consuming limited quotas. Version 1.11.0 fixes the issue.	N/A	More Details
CVE-2025-68428	jsPDF is a library to generate PDFs in JavaScript. Prior to version 4.0.0, user control of the first argument of the loadFile method in the node.js build allows local file inclusion/path traversal. If given the possibility to pass unsanitized paths to the loadFile method, a user can retrieve file contents of arbitrary files in the local file system the node process is running in. The file contents are included verbatim in the generated PDFs. Other affected methods are \`addImage\`, \`html\`, and \`addFont\`. Only the node.js builds of the library are affected, namely the \`dist/jspdf.node.js\` and \`dist/jspdf.node.min.js\` files. The vulnerability has been fixed in jsPDF@4.0.0. This version restricts file system access per default. This semver-major update does not introduce other breaking changes. Some workarounds areavailable. With recent node versions, jsPDF recommends using the \`--permission\` flag in production. The feature was introduced experimentally in v20.0.0 and is stable since v22.13.0/v23.5.0/v24.0.0. For older node versions, sanitize user-provided paths before passing them to jsPDF.	N/A	More Details
CVE-2025-68436	Craft is a platform for creating digital experiences. In versions 5.0.0-RC1 through 5.8.20 and 4.0.0-RC1 through 4.16.16, authenticated users on a Craft installation could potentially expose sensitive assets via their user profile photo via maliciously crafted requests. Users should update to the patched versions (5.8.21 and 4.16.17) to mitigate the issue.	N/A	More Details
CVE-2025-68437	Craft is a platform for creating digital experiences. In versions 5.0.0-RC1 through 5.8.20 and 4.0.0-RC1 through 4.16.16, the Craft CMS GraphQL \`save_<VolumeName>_Asset\` mutation is vulnerable to Server-Side Request Forgery (SSRF). This vulnerability arises because the \`_file\` input, specifically its \`url\` parameter, allows the server to fetch content from arbitrary remote locations without proper validation. Attackers can exploit this by providing internal IP addresses or cloud metadata endpoints as the \`url\`, forcing the server to make requests to these restricted services. The fetched content is then saved as an asset, which can subsequently be accessed and exfiltrated, leading to potential data exposure and infrastructure compromise. This exploitation requires specific GraphQL permissions for asset management within the targeted volume. Users should update to the patched 5.8.21 and 4.16.17 releases to mitigate the issue.	N/A	More Details
	Craft is a platform for creating digital experiences. Versions 5.0.0-RC1 through 5.8.20 and 4.0.0-RC1 through 4.16.16 are vulnerable to potential authenticated Remote Code Execution via Twig SSTI. For this to work, users must have administrator access to the		

CVE-2025-68454	Craft Control Panel, and allowAdminChanges must be enabled, which is against Craft CMS' recommendations for any non-dev environment. Alternatively, a non-administrator account with allowAdminChanges disabled can be used, provided access to the System Messages utility is available. It is possible to craft a malicious payload using the Twig `map` filter in text fields that accept Twig input under Settings in the Craft control panel or using the System Messages utility, which could lead to a RCE. Users should update to the patched versions (5.8.21 and 4.16.17) to mitigate the issue.	N/A	More Details
CVE-2025-68455	Craft is a platform for creating digital experiences. Versions 5.0.0-RC1 through 5.8.20 and 4.0.0-RC1 through 4.16.16 are vulnerable to potential authenticated Remote Code Execution via malicious attached Behavior. Note that attackers must have administrator access to the Craft Control Panel for this to work. Users should update to the patched versions (5.8.21 and 4.16.17) to mitigate the issue.	N/A	More Details
CVE-2025-68456	Craft is a platform for creating digital experiences. In versions 5.0.0-RC1 through 5.8.20 and 3.0.0 through 4.16.16, unauthenticated users can trigger database backup operations via specific admin actions, potentially leading to resource exhaustion or information disclosure. Users should update to the patched versions (5.8.21 and 4.16.17) to mitigate the issue. Craft 3 users should update to the latest Craft 4 and 5 releases, which include the fixes.	N/A	More Details
CVE-2025-34377	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-0625	Multiple D-Link DSL gateway devices contain a command injection vulnerability in the dnscfg.cgi endpoint due to improper sanitization of user-supplied DNS configuration parameters. An unauthenticated remote attacker can inject and execute arbitrary shell commands, resulting in remote code execution. The affected endpoint is also associated with unauthenticated DNS modification (“DNSChanger”) behavior documented by D-Link, which reported active exploitation campaigns targeting firmware variants of the DSL-2740R, DSL-2640B, DSL-2780B, and DSL-526B models from 2016 through 2019. Exploitation evidence was observed by the Shadowserver Foundation on 2025-11-27 (UTC). Affected devices were declared end-of-life/end-of-service in early 2020.	N/A	More Details
CVE-2025-34380	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-69224	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below of the Python HTTP parser may allow a request smuggling attack with the presence of non-ASCII characters. If a pure Python version of AIOHTTP is installed (i.e. without the usual C extensions) or AIOHTTP_NO_EXTENSIONS is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. This issue is fixed in version 3.13.3.	N/A	More Details
CVE-2025-69226	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below enable an attacker to ascertain the existence of absolute path components through the path normalization logic for static files meant to prevent path traversal. If an application uses web.static() (not recommended for production deployments), it may be possible for an attacker to ascertain the existence of path components. This issue is fixed in version 3.13.3.	N/A	More Details
CVE-2025-34375	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below contain parser logic which allows non-ASCII decimals to be present in the Range header. There is no known impact, but there is the possibility that	N/A	More

69225	there's a method to exploit a request smuggling vulnerability. This issue is fixed in version 3.13.3.		Details
CVE-2025-69227	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow for an infinite loop to occur when assert statements are bypassed, resulting in a DoS attack when processing a POST body. If optimizations are enabled (-O or PYTHONOPTIMIZE=1), and the application includes a handler that uses the Request.post() method, then an attacker may be able to execute a DoS attack with a specially crafted message. This issue is fixed in version 3.13.3.	N/A	More Details
CVE-2025-69228	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a request to be crafted in such a way that an AIOHTTP server's memory fills up uncontrollably during processing. If an application includes a handler that uses the Request.post() method, an attacker may be able to freeze the server by exhausting the memory. This issue is fixed in version 3.13.3.	N/A	More Details
CVE-2025-69229	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. In versions 3.13.2 and below, handling of chunked messages can result in excessive blocking CPU usage when receiving a large number of chunks. If an application makes use of the request.read() method in an endpoint, it may be possible for an attacker to cause the server to spend a moderate amount of blocking CPU time (e.g. 1 second) while processing the request. This could potentially lead to DoS as the server would be unable to handle other requests during that time. This issue is fixed in version 3.13.3.	N/A	More Details
CVE-2025-69230	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. In versions 3.13.2 and below, reading multiple invalid cookies can lead to a logging storm. If the cookies attribute is accessed in an application, then an attacker may be able to trigger a storm of warning-level logs using a specially crafted Cookie header. This issue is fixed in 3.13.3.	N/A	More Details
CVE-2025-34374	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34379	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2026-0621	Anthropic's MCP TypeScript SDK versions up to and including 1.25.1 contain a regular expression denial of service (ReDoS) vulnerability in the UriTemplate class when processing RFC 6570 exploded array patterns. The dynamically generated regular expression used during URI matching contains nested quantifiers that can trigger catastrophic backtracking on specially crafted inputs, resulting in excessive CPU consumption. An attacker can exploit this by supplying a malicious URI that causes the Node.js process to become unresponsive, leading to a denial of service.	N/A	More Details
CVE-2025-68954	Pterodactyl is a free, open-source game server management panel. Versions 1.11.11 and below do not revoke active SFTP connections when a user is removed from a server instance or has their permissions changes with respect to file access over SFTP. This allows a user that was already connected to SFTP to remain connected and access files even after their permissions are revoked. A user must have been connected to SFTP at the time of their permissions being revoked in order for this vulnerability to be exploited. This issue is fixed in version 1.12.0.	N/A	More Details
CVE-2025-52517	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. A race condition in the issimian device driver results in a double free, leading to a denial of service.	N/A	More Details
	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Coolify versions prior to and including v4.0.0-beta.420.8 have an information disclosure vulnerability in the \`/api/v1/teams/{team_id}/members\` and		

CVE-2025-59955	`/api/v1/teams/current/members` API endpoints allows authenticated team members to access a highly sensitive `email_change_code` from other users on the same team. This code is intended for a single-use email change verification and should be kept secret. Its exposure could enable a malicious actor to perform an unauthorized email address change on behalf of the victim. As of time of publication, no known patched versions exist.	N/A	More Details
CVE-2025-34390	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34389	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2024-56809	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2024. Notes: none	N/A	More Details
CVE-2024-56825	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2024. Notes: none	N/A	More Details
CVE-2025-34388	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34387	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34386	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34385	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34384	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34381	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-69290	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2025. Notes: none	N/A	More Details
CVE-2025-69291	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2025. Notes: none	N/A	More Details
CVE-2025-64421	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions up to and including v4.0.0-beta.434, a low privileged user (member) can invite a high privileged user. At first, the application will throw an error, but if the attacker clicks the invite button a second time, it actually works. This way, a low privileged user can invite themselves as an administrator to the Coolify instance. After the high privileged user is invited, the attacker can initiate a password reset and log in with the new admin. As of time of publication, it is unclear if a patch is available.	N/A	More Details

CVE-2025-34383	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34382	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-64422	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify vstarting with version 4.0.0-beta.434, the /login endpoint advertises a rate limit of 5 requests but can be trivially bypassed by rotating the X-Forwarded-For header. This enables unlimited credential stuffing and brute-force attempts against user and admin accounts. As of time of publication, it is unclear if a patch is available.	N/A	More Details
CVE-2025-64423	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions up to and including v4.0.0-beta.434, a low privileged user (member) can see and use invitation links sent to an administrator. When they use the link before the legitimate recipient does, they are able to log in as an administrator, meaning they have successfully escalated their privileges. As of time of publication, it is unclear if a patch is available.	N/A	More Details
CVE-2025-64424	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions up to and including v4.0.0-beta.434, a command injection vulnerability exists in the git source input fields of a resource, allowing a low privileged user (member) to execute system commands as root on the Coolify instance. As of time of publication, it is unclear if a patch is available.	N/A	More Details
CVE-2025-64425	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions up to and including v4.0.0-beta.434, an attacker can initiate a password reset for a victim, and modify the host header of the request to a malicious value. The victim will receive a password reset email, with a link to the malicious host. If the victim clicks this link, their reset token is sent to the attacker's server, allowing the attacker to use it to change the victim's password and takeover their account. As of time of publication, it is unclear if a patch is available.	N/A	More Details
CVE-2026-21439	badkeys is a tool and library for checking cryptographic public keys for known vulnerabilities. In versions 0.0.15 and below, an attacker may inject content with ASCII control characters like vertical tabs, ANSI escape sequences, etc., that can create misleading output of the badkeys command-line tool. This impacts scanning DKIM keys (both --dkim and --dkim-dns), SSH keys (--ssh-lines mode), and filenames in various modes. This issue is fixed in version 0.0.16.	N/A	More Details
CVE-2025-34373	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34268	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34327	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34345	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34344			
CVE-2025-34343	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34342	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34341	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34340	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34339	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-12793	An uncontrolled DLL loading path vulnerability exists in AsusSoftwareManagerAgent. A local attacker may influence the application to load a DLL from an attacker-controlled location, potentially resulting in arbitrary code execution. Refer to the ' Security Update for MyASUS' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-34338	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34326	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34346	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34325	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34321	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34296	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34295	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34289	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34285	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34279	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34276	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34275	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-20802	In geniezone, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10238968; Issue ID: MSV-4914.	N/A	More Details
CVE-2025-34347	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34372	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34362	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34371	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34370	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34369	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34368	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34367	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34366	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34365	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34364	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a	N/A	More

34363	vulnerability disclosure.		Details
CVE-2025-34361	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34348	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34360	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34359	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34358	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34357	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34356	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34355	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34354	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34353	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34349	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34970	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34968	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34585	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34967	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34706	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34707	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34708	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34709	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34710	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34711	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34712	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34713	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34714	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34715	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34716	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34717	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34718	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34719	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34720	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34721	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34722	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34723	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34724	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34725	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34726	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34705	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34704	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34703	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34691	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34682	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34683	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34684	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34685	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34686	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34687	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a	N/A	More

34688	vulnerability disclosure.		Details
CVE-2025-34689	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34690	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34692	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34583	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34693	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34694	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34695	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34696	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34697	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34698	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34699	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34700	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34701	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34727	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34728	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34729	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34764	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34755	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34756	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34757	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34758	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34759	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34760	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34761	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34762	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34763	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34765	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34753	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34766	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34767	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34768	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34769	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34770	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34771	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34772	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34773	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34774	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34754	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34752	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34730	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34740	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34731	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34732	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34733	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34734	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34735	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a		More

2025-34736	vulnerability disclosure.	N/A	Details
CVE-2025-34737	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34738	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34739	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34741	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34751	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34742	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34743	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34744	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34745	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34746	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34747	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34748	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34749	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34750	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34681	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34680	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34679	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34619	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34610	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34611	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34612	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34613	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34614	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34615	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34616	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34617	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34618	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34620	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34608	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34621	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34622			
CVE-2025-34623	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34624	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34625	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34626	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34627	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34628	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34629	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34609	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34607	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34631	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34595	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34586	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34587	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34588	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34589	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-			

2025-34590	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34591	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34592	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34593	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34594	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34596	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34606	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34597	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34598	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34599	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34600	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34601	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34602	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34603	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34604	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34605	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34630	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34632	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34678	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34667	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34658	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34659	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34660	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34661	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34662	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34663	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34664	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34665	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34666	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34668	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34656	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34669			
CVE-2025-34670	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34671	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34672	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34673	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34674	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34675	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34676	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34677	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34657	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34655	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34633	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34643	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34634	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34635	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34636	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34637	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34638	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34639	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34640	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34641	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34642	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34644	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34654	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34645	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34646	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34647	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34648	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34649	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34650	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34651	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34652	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34653	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34775	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34776	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34777	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34908	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34899	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34900	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34901	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34902	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34903	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34904	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34905	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34906	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34907	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34909	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a	N/A	More

34897	vulnerability disclosure.		Details
CVE-2025-34910	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34911	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34912	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34913	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34914	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34915	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34916	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34917	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34918	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34898	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34896	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34920	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34884	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34875	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34876	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-			

2025-34877	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34878	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34879	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34880	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34881	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34882	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34883	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34885	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34895	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34886	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34887	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34888	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34889	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34890	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34891	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34892	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34893	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34894	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34919	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34921	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34873	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34956	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34947	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34948	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34949	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34950	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34951	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34952	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34953	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34954	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34955	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34957	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34945	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34958	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34959	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34960	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34961	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34962	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34963	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34964	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34965	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34966	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34946	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34944	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34922	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34932	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34923	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34924			
CVE-2025-34925	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34926	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34927	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34928	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34929	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34930	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34931	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34933	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34943	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34934	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34935	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34936	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34937	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34938	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34939	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-			

2025-34940	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34941	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34942	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34874	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34872	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34778	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34812	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34803	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34804	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34805	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34806	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34807	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34808	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34809	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34810	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34811	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34813	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34801	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34814	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34815	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34816	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34817	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34818	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34819	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34820	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34821	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34822	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34802	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34800	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34824	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34788	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34779	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34780	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34781	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34782	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34783	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34784	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34785	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34786	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34787	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34789	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34799	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34790	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34791	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34792	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34793	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34794	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a	N/A	More

34795	vulnerability disclosure.		Details
CVE-2025-34796	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34797	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34798	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34823	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34825	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34871	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34860	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34851	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34852	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34853	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34854	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34855	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34856	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34857	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34858	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

CVE-2025-34859	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34861	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34849	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34862	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34863	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34864	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34865	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34866	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34867	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34868	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34869	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34870	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34850	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34848	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34826	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details

34836			
CVE-2025-34827	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34828	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34829	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34830	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34831	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34832	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34833	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34834	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34835	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34837	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34847	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34838	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34839	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34840	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34841	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-	Rejected reason: This CVE ID was rejected because it was reserved but not used for a		More

2025-34842	vulnerability disclosure.	N/A	Details
CVE-2025-34843	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34844	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34845	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34846	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details
CVE-2025-34702	Rejected reason: This CVE ID was rejected because it was reserved but not used for a vulnerability disclosure.	N/A	More Details